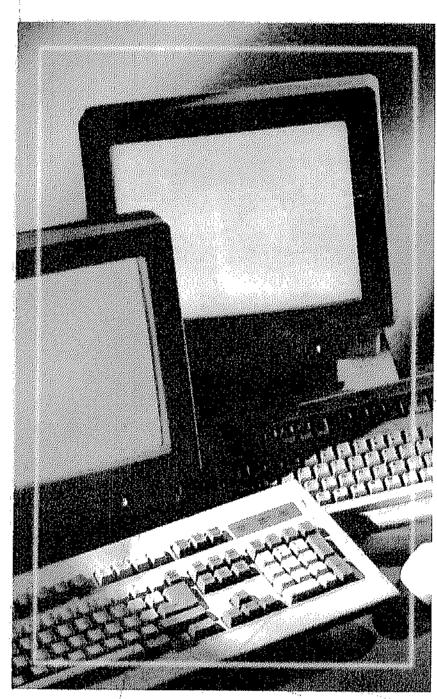


سلسلة الرضا للإنترنت 2

شبكات الإنترانت

بنيتها الأساسية وانعكاساتها على المؤسسات



م. حسام الملحم د. عمار خير بك





دار الرضا للنشر

شبكات الإنترانت

بنيتها الأساسية وانعكاساتها على المؤسسات

إعـــداد

م. حسام الملحم

د. عمّار خيربك

سلسلة الرضا للإنترنت

-٢-

سلسلة الرضا للمعلومات ٥٩

سلسلة علمية متميزة لنشر ثقافة الإدارة الحديثة والمعلوماتية بغية تطوير المؤسسات والشركات التي تسعى للريادة.

دار الرضا للنشـــر

تجهيــز – قــرب فندق برج الفــردوس – هــاتف: ٢٢٢٤٦١٧

تلفاكس: ٢٢٢٢١٦٣

ص.ب: ٤٢٦٧

E-mail: Reda-Center @ net.sy

الإشراف على سلسلة الانترنت: د. عمّار خير بك

د. راضي خازم

نيسان ٢٠٠٠

تقديم الناشر

تعتبر الشركات اليوم هي النشاط الإنساني المنظم الأهم عالمياً لإنجاز المهام والأعمال والخدمات بمختلف أنواعها بهدف الربح أو بدونه لتحقيق أهداف محددة، وخصوصاً بعد أن نجحت نظم المعلومات في التطور والانتشار العالمي، وهذا ما جعل نموذج المؤسسة أساسياً في عصر الانفجار المعرفي والمعلوماتي والتغيرات التقنية المتسارعة، ولا أدل على ذلك من أن الشركات العابرة للقارات لم تعد تخاف كبر عدد موظفيها وفروعها، وتقوم بالاتحاد والتحالف لبناء شركات أكبر لوجود تقنيات تساهم في التواصل وتطوير العمل عبر شبكات حاسوبية موثوقة وأمينة، ترفع أداء المؤسسات مهما ازداد حجمها، لدرجة أن ألف شركة عالية عابرة للقارات تسيطر على ٥٢٪ من حجم التجارة العالمية، مما شكل حافزاً لأي شركة أن تمارس عملاً عالمياً وتسوقه بين أركان الكرة الأرضية التي أصبحت قرية صغيرة، بفضل تطور طرق الاتصال، ولاسيما الشبكات الحاسوبية بنموذج انترانت.

واليوم في عصر انتشار الانترنت وتحولها إلى شبكة معلومات عالية تحوي كنوز المعرفة العالمية الديناميكية التغير والمستمرة النمو والتحديث، وبعد أن تضاعف عدد مستخدميها بشكل أسي خلال السنوات المعدودة السابقة، وبعد أن وصل عدد مستخدميها لأكثر من ثلاثمائة مليون مستخدم، تدخل الإنترنت الشركات من باب عصب العمل والتطوير وسريان وتدفق المعلومات ودورها في اتخاذ القرار، وهنا تبرز أهمية معلومات الشركة كبنك معلومات خاص يمكن لكل العاملين في المؤسسات الاستفادة منه حسب اختصاصهم وصلاحياتهم، ولا يمكن لغير العاملين في هذه المؤسسة التعامل مع هذا النظام المعلوماتي، وهذا ما أدى لظهور نموذج داخلي أو خاص للإنترنت، دعي الانترانت والذي ظنه الناس في البداية خطأ مطبعياً، وفعلاً بدأت معظم الشركات والمؤسسات تنظم معلوماتها بما يتناسب مع معايير الانترنت التي تتميز بالأمان والمرونة وسهولة التواصل وتنوع المعلومات المتبادلة، مما أدى لتفاعل أكبر وأسرع من قبل الشركات مع نموذج انترانت لبساطتها وخدماتها المتنوعة للشركات وسماحها للعاملين بدخول الشبكة عبر الاتصال الخارجي حسب السماحيات وكلمات السر ومراقبة دخول أي شخص للشبكة ومراقبة التأثيرات التي يتركها على المعلومات.

إن للانترانت انعكاس كبير على الشركات من ناحية تحسين الاتصال والتواصل بين العاملين وأمان المعلومات وطريقة عرض معلومات الشركة وأنظمتها والدعوة إلى الاجتماعات، وتجعل التعامل مع

المعلومات غنياً وإبداعياً للعاملين، ويساعد في التنسيق والترابط، والتشارك في المعلومات وإدراك التفاصيل والإحصائيات، وعرض أنظمة الشركة وخبراتها، والتغلب على صعوبات التواصل في المؤسسات الكبيرة، كما تزيد الفعالية في العمل وتحسن الأداء وصوابية القرار، وهذا ما يجعل مستقبل الانترانت هو النموذج الأمثل لتطوير أنظمة المعلومات في المؤسسات.

إن مفاهيم انترانت تكسر الحاجز في تبادل المعلومات وخدماتها وتوزع آلية اتخاذ القرار وتعتمد على إبداع العاملين بشكل أوسع، وهذا جعل شبكات الانترانت تنتشر في الشركات أكثر من أنظمة الأتمتة الشاملة لنشاطات المؤسسة، وتتحول إلى مفهوم أشمل في تبادل المعلومات يفوق مفهوم الأتمتة الإدارية، وهذا ما استطاع الدكتور عمار خيربك والمهندس حسام اللحم طرحه في هذا المرجع المتميز والهام في سلسلة الرضا للإنترنت، هذه السلسلة الحديثة والمواكبة لتطورات الشبكة العالمية انترنت وعلومها واستحقاقات استثمارها التي ستكون محور التطوير الأساسي في معظم بلدان العالم، وستكون محط الجهود العلمية لنخبة المجتمعات لسنوات عديدة، وهذا ما يجعل أهمية النشر في مجال علوم انترنت واستثماراتها حيوياً وهاماً للمكتبة العربية، لخلق تجاوب سريع مع هذه العلوم والتقنيات، تساعد في حشد الخبرات وتوجيه الطاقات في هذا الاتجاه، فالانترنت ليست استحقاقاً فقط في تسهيل وتطوير انتشارها وخدماتها، بل تشكل فرصة للتواصل العربي وتحقيق السوق العربية المشتركة الإلكترونية، بالإضافة لتحسين التواصل الثقافي والعلمي بين البلدان العربية، من هنا نتمنى لهذا المرجع الجديد من سلسلة الرضا للانترنت النجاح وتقديم الفائدة العلمية والفكرية الناجعة لكل القارئين والمهتمين، وأن تستمر هذه السلسلة على هذا المستوى العلمي، والله ولي التوفيق والنجاح.

دمشق في ١٠/٤/٢٠٠٠

دار الرضا للنشر

هاني شحادة الخوري

مقدمة الكتاب

تقدم الإنترانت وفق أبسط نموذج لها مكاناً لوضع كافة المعلومات التعاونية في المؤسسات والمنظمات التي تستخدم هذه التكنولوجيا، كما تقدم في شكلها الأكثر تعقيداً بيئة ملائمة لتطبيقات المحادثة عبر الوب في الزمن الحقيقي والتبادل الفيديوي عبر الشبكة. وما بين هذين الشكلين فإن الإنترانت تسمح بمكاملة التطبيقات التعاونية، إضافةً إلى تطبيقات الاتصالات وتبادل معلومات العمل، وبغض النظر عن مستوى التعقيد فإن الإنترانت تقدم حلولاً غير محدودة للجهد المبذول في المؤسسات التعاونية للتوفيق بين سير العمل من جهة وقنوات الاتصال من جهة أخرى، لتحسين بيئة العمل وجعلها أكثر فاعلية.

وستبقى الحاجة إلى الاتصالات الداخلية وإلى معرفة رغبات الزبائن على القدر نفسه من الأهمية الذي كانت عليه في الماضي، وستستمر الإنترانت في سد هذه الحاجة الثابتة باطراد، إذ تسمح الإنترانت لأي مجال من مجالات الأعمال (بغض النظر عن أنواع السلع التي ينتجها أو عن حجمها) بتقوية الخبرات الفكرية لكل الموظفين ونقلها إلى الزبائن، الأمر الذي يؤدي إلى توسيع قاعدة المعرفة لكل شخص له علاقة بالعمل تدريجياً.

تأتي قوة الإنترانت من الإنترنت بحد ذاتها، حيث يكمن نجاح الإنترانت في هذه القوة. في الواقع إن انتشار وسيطرة الإنترنت والتطبيقات البرمجية العاملة عليها والتي نتجت عن نجاح الإنترنت وشعبيتها هي التي أنتجت الإنترانت وهيأت مستقبلها المتألق. إلا أن الإنترانت تتميز عن الإنترنت في مساحة التغطية الجغرافية، ففي حين لا توجد أي سلطة أو تنظيم مركزي يحكم شبكة الإنترنت، حيث أنه بمقدور أي شخص على دراية كافية بالحواسيب والبرمجة ويستطيع تحمل نفقة حساب (Account) على الإنترنت أن يضع صفحة وب خاصة به على الشبكة، فإن الأمور تختلف بالنسبة

للإنترانت، فهناك بيئة معينة لتنظيم المعلومات والاتصالات ضمن العمل، وتعكس الإنترانت هذا التنظيم السائد في المؤسسة والذي قد يكون منسجماً مع الأشكال التقليدية كما هو الحال في المؤسسات ذات البنية الهرمية الرأسية، أو متوافقاً مع النموذج الجديد الذي يرتكز على مفهوم فريق العمل.

صُمِّم هذا الكتاب لمساعدة القارئ على فهم (ومن ثم التمكُّن من) قوة استثمار وتصميم شبكة إنترانت، إذ يقدّم المعلومات المطلوبة لكل من يبني شبكة إنترانت لأول مرة، أو لمدير الشبكة الذي يبحث دائماً عن طرق جديدة لتعزيز وتحسين شبكة إنترانت موجودة مسبقاً. كما أن هذا الكتاب موجّه للأشخاص الذين يعملون في أي مجال من مجالات الأعمال ـ منظمة أو عمل تجاري صغير أو جامعة أو وكالة حكومية أو شركة تجارية ـ ويستخدمون شبكات الإنترانت في تسيير أعمالهم.

ما الذي سيحصل عليه القارئ

نهدف من وراء هذا الكتاب إلى أن نقدم لأي قارئ زاداً متكاملاً من الأفكار حول ما يمكن للإنترانت أن تقدم، إضافةً إلى كيفية الاستفادة من وظيفة الإنترانت. كما نقدم طريقاً يذهب بالقارئ من المستوى المفهومي إلى الإنترانت العاملة، ومن الواضح أننا لن نستطيع أن نقدم كل التفاصيل ولكننا سنقدّم الموارد والبنية التحتية كي يستطيع القارئ معرفة كيف يصوغ الأسئلة التي سيطرحها وأين يجد الأجوبة عليها فيما يتعلق بالإنترانت.

تنظيم الكتاب

يقسم الكتاب إلى سبعة فصول:

نقدّم في الفصل الأول الإنترانت من وجهة نظر تحديد أين تنتهي الإنترنت وأين تبدأ الإنترانت، ومن ثم نناقش استخدامات موارد المعلومات المتنوعة للإنترانت.

نناقش في الفصل الثاني الشبكات المحلية التي هي البنية التحتية لشبكات الإنترانت ومن متطلبات الوصول إلى الإنترنت.

نعرض في الفصل الثالث متطلبات بناء شبكة إنترانت إذا توفرت البنية التحتية المادية، وذلك بمناقشة المتطلبات في التجهيزات المادية والبرمجية ومتطلبات الزبون، وفي هذا الفصل نعرض لمفهوم الزبون/مخدّم ومتطلبات تحقيقه في شبكات الإنترانت.

يتخصص الفصل الرابع بتوضيح المبادئ الأساسية والتقنيات المتبعة في حماية شبكات الإنترانت من مختلف أنواع الاختراقات، وضرورة اتباع سياسة أمنية محددة وواضحة تعكس احتياجات المؤسسة.

يتألف الفصل الخامس من عدة فقرات، نناقش في كل منها إحدى الخدمات الأساسية الواجب توفرها في شبكات الإنترانت، وذلك بعرض عام للخدمة ومن ثم لمتطلبات تحقيقها المادية والبرمجية.

نناقش في الفصل السادس انعكاسات الإنترانت على الشركات، وذلك من حيث المتطلبات الإضافية وأثر بناء الإنترانت على هيكلية الشركة وإنتاجيتها.

وأخيراً في الفصل السابع ننظر في مستقبل الإنترانت من خلال مناقشة الميول والاتجاهات التكنولوجية الحالية وأثرها المتوقع على شبكات الإنترانت.

المؤلفان

دمشق في 2000/3/15



فهرس المحتويات

الفصل الأول

الإنترنت والإنترانت

1-1 تعاريف أساسية

الإنترانت (Intranet) هي شبكة محلية داخلية مستقلة بحد ذاتها، ويمكن اعتبارها شبكة تعاونية (تشاركية)، أو شبكة مؤسسات تربط بين مستخدميها باستخدام تقنيات الإنترنت، فهي مبنية على أساس البروتوكولات TCP/IP المستخدمة في شبكة الإنترنت كما أنها كثيرة الشبه بها من الناحية البنيوية، إلا أنها تتميز بأنها تحد من سلطات الإنترنت اللامحدودة، فهي تمكن المستخدمين من الاتصال فيما بينهم بحرية ولكن ضمن قطاعات محكومة بسماحيات وصول قابلة للتحكم.

تجري غالباً عملية بناء وإدارة شبكة الإنترانت في مؤسسة ما من قبل شركات متخصصة أو مؤسسات معينة تُسمى أحياناً بالشركات الراعية أو الممولة (Sponsor)، ويمكن لهذه الشبكة الاتصال مع شبكة الإنترنت العالمية مما يسمح بالاتصال بين مختلف البنى المادية للأنظمة الحاسوبية بين المستخدمين اتصالاً آنياً

إن شبكات الإنترانت ليست فكرة جديدة تبحث عن التطبيق على أرض الواقع. إذ يمكن النظر إلى بعض تطبيقات الإنترنت على أنها تطبيقات واسعة النطاق لشبكة إنترانت (مثل: America On-line

<AOL> أو Bulletin Board Systems <BBSs>)، حيث تربط هذه التطبيقات بين مجموعة معينة من المستخدمين الذين يدخلون إلى مواقع إنترنت عن طريق كلمة سر أو أي تقنية أخرى مستخدمة للتعرف عليهم.

على سبيل المثال هناك حساب خاص لكل مستخدم يسجل في AOL ويتم الوصول إليه عن طريق كلمة سر معينة. يسمح نظام كلمات السر للمستخدمين بانتقاء الخصائص التي تهمهم، أي بتقليص الخدمات وعدد المعاملات التي يجب المشاركة بها لتلبية المتطلبات الشخصية. من جهة أخرى يسمح النظام لمزودي الخدمات بمعرفة مدى حجم الاستخدام من قبل المسجلين لديهم، وكذلك بالحصول على معلومات حول الحساب والدفع.

على النقيض من هذه الخدمات التجارية الواسعة، فإننا سنناقش في هذا الكتاب شبكات الإنترانت المبنية من قبل ولأجل مجموعات محددة من المستخدمين. حيث أن هذه الشبكات أصغر من حيث المساحة الجغرافية، ولكنها أكثر تخصصاً، وأكثر تعقيداً في الخدمات التي تقدمها، ومن جهة أخرى، وبالنظر إلى استخدامات شبكات الإنترانت كوسيلة اتصال داخلية، فإن شبكات الإنترانت تتميز باعتمادها على العديد من تقنيات أمن الشبكات أثناء تصميمها.

يكمن الاختلاف الأساسي بين تطبيقات الإنترنت السابقة الذكر، وشبكة الإنترانت الخاصة بمؤسسة معينة في البنية، وفي الغاية المطلوبة. وعلى الرغم من أن المفاهيم الأساسية هي نفسها، فإن الاختلاف من وجهة نظر معينة هو في الكم مقابل النوع. إذ تميل الخدمات السابقة ـ الموجهة للمستهلكين على مساحة واسعة ـ إلى تقديم كل الأشياء إلى كل المستخدمين لأي سبب كان، في حين تركز شبكة الإنترانت الخاصة بشركة معينة الاهتمام بمجموعة محدودة من المستخدمين حيث تتيح طيفاً محدداً من الإمكانات لتحقيق أهداف هذه الشركة.

من الأخطاء الشائعة عند الحديث عن شبكات الإنترانت، هو النظر إليها كبريد إلكتروني، فمن المعروف أن تطبيقات البريد الإلكتروني والإنترانت تشترك في مزايا عامة ؛ مثلاً كل منهما يقدم خدمة الاتصال بشكل مخصص، وكل منهما يسمح بتبادل الرسائل. لكن الإنترانت تختلف جوهرياً بميزة

تواجدها على بنية تشابه شبكة الإنترنت العالمية. بالنتيجة فإن الإنترانت أكثر تعقيداً وتغيراً من البريد الإلكتروني الثابت نوعاً ما.

يستخدم البريد الإلكتروني من حيث المبدأ نظاماً مركزياً للتوجيه، وذلك لجعل الاتصالات خطية ومتتابعة بين المستخدمين. بينما تعمل الإنترانت باستخدام تقنيات الإنترنت، وهذا يعني إمكانية تفاعل الكثير من المستخدمين فيما بينهم في نفس الوقت، وإمكانية التخزين والبحث في الوثائق وكذلك التشارك على الملفات، وتبادل الرسومات، والصوت، والفيديو. وتُصمّم الإنترانت بطريقة تمكن المستخدمين من الوصول إلى الشبكة العنكبوتية العالمية (أو الوب اختصاراً World Wide Web <WWW>) عبر الإنترانت وصولاً شفافاً، أي بدون أن يلاحظ المستخدم أنه ينتقل من الإنترانت إلى الإنترنت وبالعكس.

1-2 مزايا الإنترانت

تقدم الإنترانت العديد من المزايا للمؤسسات، ويمكن أن نصنف هذه المزايا في المجموعتين الواسعتين التاليتين:

- الفعالية، ونقصد بها: تحسين تقنيات تبادل المعلومات من حيث التغلب على الصعوبات المنطقية في جمع ونشر المعلومات الضرورية بطريقة آنية.
- الفاعلية، ونعني بها: التضارب التنظيمي الذي قد ينجم بين العملية التعاونية في المؤسسة وعملية اتخاذ القرار.

1-2-1 تحسين الفعالية

يرتبط تحسين الفعالية بقياسات كمّية، فعلى سبيل المثال: هناك العديد من الدراسات بخصوص الإنترانت توضّح التوفير في المصاريف الزائدة (مثل الرسائل البريدية أثناء الليل، أجرة البريد، نفقات

الاتصالات الهاتفية البعيدة)، وكذلك يأتي التوفير من تقليل الاعتماد على المطبوعات "المنتجة" في الشركة، مثل كتب الإرشاد حول الشركة، أو المنشورات عن المنتجات أو عن العلاقات مع الزبائن، التي يمكن نشرها إلكترونياً، بدلاً من طباعتها وإرسالها بالبريد.

وهكذا فإن تحسين الفعالية يعني التوفير في وقت العاملين في الشركة، حيث تقلل شبكة الإنترانت المهيأة تهيئاً كاملاً من الوقت الضائع في تبادل العديد من مسودات الوثائق، وكذلك من الوقت المهدور في تنسيق عمليات جمع المعلومات.

يمكن أن نطرح الأمثلة الواقعية التالية:

1- تسهل الإنترانت على نحو كبير عملية المراجعة في منشورات البحث التكنولوجي الخاصة بالمؤسسات، عن طريق تأمين النشر السريع وأتمتة عملية معالجة الأجوبة والملاحظات.

2- تفيد الإنترانت في العديد من المؤسسات في إدارة نشر الأخبار، حيث تجري عمليات إضافة الأخبار الجديدة وإزالة القديمة وتدوير المواضيع الأخبارية بشكل إلكتروني (في الشبكة) من مكان واحد، بدلاً من أن تجري مكتبياً في عدة مكاتب في الشركة.

3- يمكن أن يستخدم قسم المبيعات في شركة ما شبكة الإنترانت الخاصة بها استخداماً فعّالاً كوسيط للعلاقات مع الزبائن، كما يمكن لممثلي قسم المبيعات أن يحصلوا على معلومات إضافية حول المنتجات بطريقة مستمرة، بدلاً من إعداد العديد من الشفافيات التوضيحية أو المطبوعات التي تشرح طبيعة المنتجات. كما يمكن أن يستفيد قسم التسويق من الإنترانت بعرض المنتجات الخاصة في الشركة عن طريق بناء موقع خاص وتزويد المستخدمين بكلمات سر للحصول على معلومات حول آخر المنتجات قيد البحث والتطوير، ومعلومات أخرى حول أمان المنتجات.

4- يمكن أن تستخدم شركة تجارية عالمية الإنترانت الخاصة بها لتنظيم جدول أعمالها المعقّد. وفي أي وقت، يمكن لهذه الشركة أن تدير الاجتماعات التقنية والمهمات ومؤتمرات الأعمال بالإضافة إلى اجتماعاتها السنوية والفصلية التي تجذب المئات من المشتركين من جميع العالم، حيث يكون لكل من هذه الاجتماعات قائمةٌ للحضور، ومخططٌ للاجتماع، وكذلك النتائج المتوقعة لكل من هذه

الاجتماعات. قبل وجود شبكة الإنترانت الخاصة بهذه الشركة، فإن إدارة المطبوعات التي تدعم هذه الاجتماعات كانت تتطلب خمسة من الموظفين بدوام كامل وتكلف آلاف الدولارات في كل سنة تُصرف في تكرار الأعمال اللازمة لتحضير هذه المطبوعات وتوزيعها، بينما بوجود شبكة الإنترانت يمكن وضع كل هذه الأمور على موقع الشركة على الإنترانت، ويتم تنظيم الوصول إليها كلياً أو جزئياً بحسب كلمة سر المستقبل.

كما يمكن أن يجري الإعلام باجتماعات الشركة وجداولها الزمنية أيضاً عبر الإنترانت، حيث يمكن وضع قائمة بكل الاجتماعات ومواعيدها مع الأمور المتعلقة بكل منها، بحيث يمكن لجميع الأعضاء أن يطّلعوا عليها بوضوح، لمعرفة التفاصيل المرغوب بها، والتسجيل الفوري للمشاركة في أي منها.

1-2-2 تحسين الفاعلية

تشجّع الإنترانت عملية تبادل المعلومات عبر الحدود التقليدية (الحدود التنظيمية والجغرافية)، وإذا أديرت جيداً فإن هذا التحسن في تبادل المعلومات يصبح نقطة البدء لتعاون كبير بين قطاعات المؤسسة التي كانت منفصلة. إن الاستخدام الخلاق للإنترانت يمكن أن يسهل عملية التطوير المؤسساتي من بنية تنظيمية تقوم على مبدأ التنظيم من الأعلى نحو الأسفل إلى بنية متنوعة أكثر مرونة، وذلك بتعزيز التفاعل المنسّق.

يمكن أن نطرح الأمثلة الواقعية التالية:

1- تستخدم شركة قانونية عالمية الإنترانت الخاصة بها لتعزيز العملية التعاونية ضمن بيئتها ؛ إذ تسمح الإنترانت لخبراء الشركة بتبادل المعلومات ـ ضمن بيئة آمنة ـ حول القضايا المطروحة لمناقشة المشاكل القانونية والتنظيمية التي تواجههم، وللحصول على استشارات زملائهم، حيث تضمن الإنترانت تحقيق هذه الأمور بسرعة وبسرية. يسمح ربط المشاركين في كل من مكاتب الشركة بالسيطرة على الخبرة الجماعية، ويطوّر معرفتهم وقدراتهم على كسب الزبائن.

2- في إحدى الشركات الكيميائية المتخصصة، تتواجد أقسام التطوير والبحث وأقسام التسويق في بلدان متعددة، مما يخلق الكثير من الصعوبات في استجابة الزبائن لعملية التطوير في المنتجات. استخدمت هذه الشركة الإنترانت الخاصة بها لتسهيل عملية التبادل المستمرة بين الأقسام السابقة ؛ فبُني نظام يشتمل على عقد اجتماعات منتظمة على الشبكة، وعلى طرح استطلاعات رأي للزبائن بمشاركة قسم البحث والتطوير، وكذلك ضمّ النظام روتين تبادل الأخبار بين الأقسام. مكّن هذا النظام الشركة من إضافة متطلبات وأفضليات الزبائن إلى عملية تطوير الإنتاج في مراحلها المبكرة، أي أصبح بإمكان الزبائن المساهمة في البحث والتطوير بفعّالية، بمعنى أن منتجات الشركة أصبحت أكثر إرضاءً لحاجات الزبائن. وبنفس الوقت أصبح بمقدور الزبائن الحصول على خبرات الشركة في مجال البحث والتطوير، وذلك عن طريق قسم التسويق الذي يطّلع على التطورات التقنية الجديدة.

3- تربط منظمة دولية ذات اهتمامات عامة المئات من مواقع الفروع عبر شبكة إنترانت وذلك ليستخدمها الساهمون في المنظمة لربط الميول التنظيمية والاجتماعية معاً. العديد من هذه الفروع صغير الحجم، لكنه مزوّد بقوائم محلية، ويعتمد أساساً على الموظفين من المتطوعين، وإذا احتاج أحد هذه الفروع إلى المصادر أو إلى عقد ندوات للممولين أو لحضور المؤتمرات لإظهار قضايا دولية فإن الإنترانت الخاصة بهم تسمح لهم بالنفاذ إلى الفروع المحلية للاستفادة من تجارب واستراتيجيات بعضهم البعض، كما تساعدهم على نشر المعلومات على مستوى جميع الأعضاء.

1-2-3 تقييم الفائدة

تبين الحالاتُ المذكورة سابقاً المقدرات الأساسية التي يمكن أن تقدمها الإنترانت. وتُبرز هذه الحالات عاملاً مهماً في تقييم الفائدة من الإنترانت: وهو المضمون.

لكل إنترانت ناجحة مضمونٌ (معلومات) يُقيِّمه المستخدمون، بالطبع تتغير طبيعة هذا المضمون تغيّراً كبيراً حسب أفضليات المجموعات الفردية من المستخدمين، ولكن يمكن تطبيق بعض المبادئ على أي

مضمون معتبر، إذ يتفق كل من ممولي الإنــترانت والمستخدمين علـى حـد سـواء أن معلومـات المواقـع يجب أن تحقق بعض المواصفات الأساسية:

- *الترابط بين المحتوى والشكل*: من وجهة نظر المستخدم وليس الممول، فالمؤسسات التي تستخدم الإنترانت كمنتدى سلبي قد تخيب آمالها في استثمارها.
- *الاستجابة الجيدة*: تُضعف شدة الطلب على الإنترانت من نسبة مشاركة المستخدمين، وقد يعود المستخدمون إلى استخدام وسائل الاتصال التقليدية عندما تصبح رسـائل الـبريد الإلكـتروني مثـلاً بطيئة أو غير موثوق بها.
- *التجديد الدوري*: يعاني العديد من مواقع الوب، سـواء أكـانت عامـة أم خاصـة، مـن المضمـون الثابت، فيتناقص الاهتمام بها ومن ثم اسـتخدامها بسـرعة. توفـر الإنـترانت إمكانيـة التجديـد الدائم للمعلومات المتغيرة، وهذه الإمكانية يجب أن تُستثمر باستخدام الخصائص القابلة للأتمتة.
- *النفاذ*: يصبح محتوى أفضل موقع في العالم معدوم القيمة إذا لم يتمكـن المسـتخدمون مـن النفـاذ إليه بسرعة وسهولة. فالمبدأ الأساسي في الإنـترانت هـو توفـير المعلومـات، وعنـد تصميـم الموقـع يجب الاستفادة من محركات البحث والتقنيات الأخرى التي تحسّن من سرعة وصول المستخدم إلى المعلومات التي يرغب بالحصول عليها.

من المهم أن نتذكر دائمـاً أن الإنـترانت موجّهـة مـن قبـل المسـتخدم (User-Driven)، وأن حاجـات المستخدم وأفضلياته يجب أن تؤخذ بعين الاعتبار في التصميـم الأولي للمواقـع والخدمـات. وكمـا هـي الحال في أي مشروع بنائي آخر فإن التخطيط لبناء الموقع في البداية أفضل من تعديله فيما بعد ليلـبي متطلبات المستخدمين. وعند التصميم الأولي يجـب إدخـال المـيزات والوظـائف الـتي تجعـل المضمـونَ حديثاً على الدوام وذا صلة، بمواصفات الموقع.

3-1 معايير الاستفادة من الإنترانت

إن القياس الأساسي في تقييم الإنترانت هو الحاجة إلى المعلومات في المؤسسة، وكقاعدة عامة فإن الإنترانت تكون أكثر فائدة للمؤسسات التي تحقق:

- سعة الانتشار جغرافياً.
- المشاركة في الأعمال العامة.
- الحاجة إلى معلومات مشتركة.
- تثمين التعاون.

وكما تبيّن هذه القائمة البسيطة، فإن معايير الاستفادة من الإنترانت هي معايير موضوعية وشخصية، كما أنها ثقافية ولوجيستية، ولكي تكون الإنترانت ذات معنى على أقل تقدير، يجب أن تركّز على محور معين ؛ وغالباً ما يكون هذا المحور عملاً عاماً، أو غرضاً تنظيمياً مشتركاً بين أفراد أو مجموعات متفرقة.

ومن الضروري أن نبقي في أذهاننا أن كل مؤسسة بحاجة إلى إنترانت.

لنفترض مثلاً أن شركة صغيرة تُدار من موقع واحد، ويجري تبادل المعلومات فيها تبادلاً كافياً من خلال المذكرات أو الاجتماعات. إن مثل هذه الشركة قد تستخدم الإنترانت كمصدر لجمع المعلومات أو الخبرات، ومن غير المحتمل أن تكون بحاجة لإنترانت بقدرات وفعالية إضافية.

على النقيض من الحالة السابقة لنأخذ مثلاً شركة تملك العديد من مكاتب المبيعات أو العديد من التقسيمات العملياتية في أكثر من موقع، أو تدير العديد من المؤسسات التجارية، أو العديد من المجموعات أو الأعضاء. تستفيد هذه الشركة استفادةً كبيرة من بناء الإنترانت الخاصة بها. حيث تُجاهد المؤسسات الفرعية لتلبية حاجات المدراء من المعلومات الشاملة والآنية، وتُرهق هذه الشركات

من التحديات اللوجيستية التي تنتج عن تواجد الفروع في مناطق زمنية مختلفة، وعن أنظمة الحاسبات غير المتوافقة، وخدمات الهاتف المحلية المزعجة.

وكنتيجة لهذه العوائق وغيرها، قد لا تُتخذ القرارات الحرجة بالاستناد على التعاون الكامل بين الشاركين الرئيسين، أو على المعلومات التحتية الشاملة التي يجب أن تتوفر على حد سواء لكل صانعي القرار، إذ يحتمل أن يكون هناك عدم تطابق في المعلومات الصادرة من مواقع الفروع أو المكاتب والمنشورة عن الأعضاء أو طاقم المؤسسة، وبطريقة مماثلة تخضع المؤسسات الواسعة الانتشار جغرافياً لصعوبات غير حتمية في ترحيل بيانات الشركة (مثل أشكال المبيعات، أو التصوّرات المالية، ...)، إلى المقر العام.

تساعد الإنترانت الأكثر قوة على خلق صورة عامة بين المكوّنات التّنظيمية المتباينة من خلال "تفويض الأفراد"، ويعتبر هذا الأمر بحد ذاته مفهوماً ثورياً بالنسبة للعديد من المؤسسات الراغبة بـ "إنجاز الأهداف الجماعية من خلال توزيع السلطة" وليس بمركزتها.

يمكن أن نضيف لهذه الرؤية الغائية لاستعمال الإنترانت العديد من الاستعمالات التي قد تكون أقل أهمية لكنها تقدم فوائدَ هامّةً، فالتباين الجغرافي مثلاً يفرض ضرورة وجود أرشيف مركزي لأمور السياسة التعاونية، وكذلك الحاجة إلى تحليلات متجددة بانتظام لنظام المعلومات، وإلى أتمتة إصدار البيانات المالية الفصلية، وإحصائيات الإنتاج، أو قوائم العضوية.

تساعد هذه الاستعمالات الأساسية في توفير الوقت بجعل عملية إصدار التقارير الروتينية أكثر انسياباً، كما أنها تضمن جاهزيّة دائمة للحصول على المعلومات الرئيسية في أية لحظة. وعلى الرغم من أنه يمكن للشبكات واسعة النطاق (Wide Area Network <WAN>) أن تلعب دور مستودع مركزي للملفات أو للبريد الإلكتروني المشترك، فإن الشبكة واسعة النطاق لا تعني بالضرورة أنها إنترانت. فهي لا تملك كامل قدرات الإنترانت، إذ تتفوق الإنترانت حتى في تصميمها الأساسي على الشبكة واسعة النطاق من حيث سهولتها وكفاءتها في تأدية وظائف عديدة.

4-1 تصميم الإنترانت

تُعتبر شبكة الإنترانت شبكة موجهة من قبل المستخدم، وهذا يعني ضرورة أن يعكس تصميمها حاجات المستخدم. لذلك فإن البداية الجيدة تكون بتحديد هذه الحاجات ضمن المؤسسة، مما يساعد على وضع أهداف واقعية بالإضافة إلى التركيز على استغلال مزايا الإنترانت.

في البداية يجب تحديد العوامل التنظيمية الكبيرة لتطبيقات الإنترانت:

1-4-1 البنية

يساعد فهم البنية التنظيمية في المؤسسة على تحديد الفائدة العامة من الإنترانت، إضافةً إلى تحديد الوظيفة التي تعطي للإنترانت القيمة العظمى، وذلك من خلال تحديد الانتشار الجغرافي للمؤسسة، والبنية التنظيمية في المؤسسة (هرمية، موزعة، مركزية، لامركزية).

2-4-1 الاتصالات الداخلية و تبادل المعلومات

يساعد فهم روتين تبادل المعلومات في المؤسسة داخلياً على إزالة الحواجز والثغرات التي يمكن أن نوجه الإنترانت لحلها:

1- ما هي المصادر الأساسية للمعلومات داخل وخارج المؤسسة ؟

2- كيف تجري عملية نقل معلومات العمل عادةً (بالبريد الإلكتروني، طرد خاص، هاتف، اجتماعات، وسائل أخرى) ؟

3- كيف تجري عملية اتخاذ القرارات ؟

4- كيف تجري قيادة عملية البحث والتشارك فيها ؟

1-4-3 الاتصالات الخارجية

يساعد فهم كيفية تفاعل المؤسسة مع محيطها على طرح فرص استخدام الإنترانت لتلبي حاجاتها بشكل أفضل.

1- هل هذه المجموعات التي تتفاعل المؤسسة معها تقع خارج المؤسسة (كالزبائن، المساهمون، المتطوعون) ؟

2- كيف تبقيهم المؤسسة على اطلاع ؟

3- ما هي المعلومات التي يحتاجونها، والتي يريدونها أو يتوقعونها ؟

4- كيف تستقبل المؤسسة المعلومات منهم وكيف تعالجها ؟

1-4-4 الصعوبات

بالنظر إلى موانع إقامة اتصالات فعالة يمكننا تحديد الضعف التنظيمي، وإسناد الأولويات إلى عملية تطوير الإنترانت.

- ما هي العقبات الأساسية لعملية تبادل معلومات فعالة ؟

2- هل هذه العقبات تقنية، لوجيستية، ثقافية ؟

3- ما مدى تأثير هذه العقبات ؟

1-4-5 المصادر

يساعد تقييم المصادر المتوفرة على تشكيل نقطة بدء لتصميم وتحقيق الإنترانت.

1- ما هو مستوى المؤسسة الحالي لقابلية الحوسبة (إدخال الحاسوب) ؟

2- ما هي المصادر البشرية اللازمة (من موظفين ومموِلين) لبناء وإدارة الإنترانت ؟

3- ما هي المصادر التقنية والمالية المتوفرة حالياً ؟

5-1 تحديد أهداف الإنترانت

كما ورد سابقاً، فمن المحتمل أن تكون أهداف الإنترانت متواضعة أو طموحة، محددة تماماً أو واسعة التعريف، وبغض النظر عن ماهية هذه الأهداف، فمن المهم أن تكون مُعرَّفة بوضوح مقدماً.

كما هي الحال في أيـة مبادرة كبيرة يجب أن تطرح المؤسسة الممولة على نفسها بعض الأسئلة الأساسية قبل المباشرة في بناء الإنترانت.

1- ما الذي نرغب في الحصول عليه من شبكة الإنترانت ؟

إن الإجابة على هذا السؤال تحدد الهدف المرجو من بناء الإنترانت.

2- لماذا نريد أن نحقق الهدف ؟

إن إجبار المؤسسة على اعتبار الإنترانت تقع ضمن سياق استراتيجية عملها الإجمالية (لأن الآخرين يقومون بذلك) ليس سبباً مقنعاً.

3- كيف نتوقع أن نحقق هذا الهدف ؟

الإجابة على هذا السؤال تساعد على وضع إطار لخطط المشروع، ويتطلّب هذا تحديد مهام القيادة، المواصفات التقنية، المصادر المطلوبة، جدول المواعيد، نماذج الموظفين.

4- كم تبلغ التكاليف المالية الضرورية لتحقيق هذا الهدف ؟

يجب أن تضم الصورةُ الكاملة لنفقات بناء الإنترانت توقعات كل من النفقات قصيرة الأمد والمدخرات المتوقعة خلال زمن التنفيذ.

5- كيف نراقب التقدم ؟

تنحو الإنترانت للتطور عبر الزمن، ومن الضروري بناء تقنيات لتحديد مدى التقدم المنجز مقارنة مع التوقعات.

6- كيف نقيّم النجاح ؟

كما في أي مبادرة أخرى، تتحدد فاعلية الإنترانت نهائياً من خلال تحليل النفقة مقابل المنفعة.

وعلى مستوى أكثر تحديداً، تحتاج المؤسسات المولة لتعريف المعايير التالية أيضاً:

آ- من هم المستخدمون المعنيون بالإنترانت ؟

يمكن أن يكون نطاق المستخدمين الأساسيين للإنترانت واسعاً أو ضيقاً حسب متطلبات المؤسسة. يمكن أن نحدد هذا النطاق مثلاً بـ "كل موظفي الشركة" أو "كل رؤساء الأقسام".

ب- كيف نتوقع أن يستخدم الجمهور الذي نستهدفه الإنترانت ؟

يتغير التفاعل مع الإنترانت إلى حد بعيد، بحسب وظائف الموقع وحاجات المستخدم. فمن أجل كل مجموعة من المستخدمين، يجب أن تحدد المؤسسة فائدة ما لتضمن أن تصميم الموقع يلبي حاجات وتوقعات المجموعة. فقد يجد المدراء المتوسطون مثلاً المنفعة العظمى في خدمة التراسل عبر مختلف البنى المادية، بينما تفضل فئة ممثلي المبيعات فكرة الأرشيف المركزي.

ج- ما الذي يجب أن يحققه الجمهور لكي يستعمل الإنترانت ؟

بعد تعريف من سيستعمل الإنترانت ولأي سبب، يجب تقييم ما هو موجود من ناحية قدرات الحواسيب، كيفية التوصيل، الخبرة المسبقة. في بعض الحالات مثلاً قد تحتاج مجموعة من المستخدمين إلى تدريب أساسي شامل، بينما يكتفي الباقون بتعلم كيفية التوصيل وقراءة دليل استثمار المستخدم.

6-1 البدء بمشروع بناء الإنترانت

قد تؤثر الطريقة التي تبدأ بها مؤسسة ما مشروع بناء شبكة الإنترانت على نجاح أو فشل هذا المشروع، ولأن الهدف الأساسي لأغلب شبكات الإنترانت هو تسهيل التعاون عبر الحدود التنظيمية، فمن المنطقي أن نبدأ من الأسس التعاونية. يعطي مشروع بناء الإنترانت فرصة طبيعية لجمع الاختصاصات المتنوعة ذات الصلة للتركيز على هدف واحد، والناتج النهائي سيكون بلا شك أفضل ممّا يمكن الحصول عليه فيما لو بقيت هذه الاختصاصات مستقلةً.

يمكن أن يبدأ الدافع لبناء الإنترانت من أي مكان في المؤسسة: دوائر المبيعات الإقليمية، مختبرات البحوث، أقسام القانون، أو أقسام السكرتارية. وبغض النظر عن مكان نشوء الفكرة، وكما هي الحال في أية مبادرة تنظيمية واسعة، فإن بناء شبكة إنترانت يتطلب قيادةً وتوجيهاً ومصادرَ ماديةً.

بكلمات أخرى فإن مشروعَ بناءِ إنترانت ناجحاً يتطلب الأمور التالية:

- مساندة وتصديق الإدارة العليا.
- رئيساً للمشروع بتفويض واضح.
- الأدوات والمصاريف الضرورية لإنجاز العمل.

إضافةً إلى ذلك، فكلما كانت القيادة والمسؤولية واضحتين، فإن مثل هذا المشروع سيستفيد استفادةً كبيرة من تنوع الاختصاصات المطلوب توفرها في الفرق المساهمة في الشروع، وهذا يساعد على أن تضمن المؤسسة ككل القيمة القصوى من استثمارها. ومن الأخطاء الشائعة إسناد عملية تطوير الإنترانت إلى قسم إدارة نظم المعلومات (Management of Information Systems <MIS>) حصراً. فعلى الرغم من أن هذا الخيار يمكن أن يبدو معقولاً إذا نظرنا إليه نظرةً سطحيةً، ولكن بسبب أسس ومبادئ الإنترانت التقنية، فإن النتائج ستكون مخيبة إذا ذهب عمل الخبراء التقنيين هباءً.

يمكن أن نقترح طريقة أفضل من ذلك، وذلك بأن نُشكِّل فريقاً يشمل طيفاً واسعاً من المستخدمين الرئيسيّين ضمن المؤسسة، ليستفيد المهندسون التقنيون من معطيات المستخدمين خلال تطويرهم لمواصفات الإنترانت.

ولكي نحصل على عملية تصميم وبناء ناجحة يجب أن ننظر في المثال التالي الذي حققته إحدى الشركات العاملة في المجال الصناعي والتي اتبعت الطريقة السابقة كما يلي:

شكل رئيس قسم فريقاً من ستة أعضاء في مشروع بناء شبكة الإنترانت تحت القيادة المباشرة لنائبه لشؤون العمليات. يتألف الأعضاء من كبار ممثلي قسم إدارة نظم المعلومات، وقسم الاتصالات، وقسم شؤون البيئة، وقسم القانون، وقسم تسويق الإنتاج، طورت هذه المجموعة بالعمل سوية لمدة شهرين، خطة عمل مفصلة لبناء شبكة الإنترانت. تضمنت هذه الخطة تعريف أهداف المشروع تعريفاً واضحاً وصريحاً، وكذلك تقييماً لاحتياجات المستخدمين، والمواصفات التقنية، ومنهج التدريب، والبرنامج الزمني لتحقيق المشروع. استدعى أعضاء الفريق موظفي المؤسسة للاستفادة من أفكارهم، عن طريق استبيانات رأي، وليعملوا كمجربين لنموذج تجريبي لموقع إنترانت، عين قسم إدارة نظم المعلومات مجموعة من المهندسين لتقوم بمهمة تصميم البنية التحتية واختيار البرمجيات المناسبة.

لم يتضمن تصميم الشبكة المواصفات التقنية فقط، بل تضمّن أيضاً خطة تفصيلية لإدارة الاتصال على الشبكة والمضمون ولتوسيع الموقع ليستوعب كامل نطاق المستخدمين. وجرت عملية بناء الشبكة أسرعَ من المتوقع جزئياً، بسبب شعبية الموقع بين المستخدمين، واستجابة فريق المشروع لملاحظات المستخدمين. بعد انتهاء المشروع تابع فريق المشروع العمل للإشراف ولضمان النوعية، ولاعتماد الميزات والوظائف الجديدة المقترحة من قبل المستخدمين ولمواكبة التقدم التقني.

بدأت هذه الإنترانت بفكرة، ومن ثم نُفذت هذه الفكرة ونجحت بتعيين إدارة لمتابعتها وفريق لتحقيقها. ودائماً يتطلب النجاح التخطيط الجيد والموارد المالية الكافية، والأهم من ذلك الالتزام المرافق للمشروع كأولوية عمل ؛ وكنتيجة لجهود هذه الأقسام، جرى تبني شبكتها كنموذج من الممكن تكراره.

7-1 الخلاصة

تقدم شبكات الإنترانت إمكانيات عظمى للمؤسسات التي تفهم إمكانياتها وترصد المختصين والمصادر لبنائها، ويمكن الحصول على هذه الإمكانيات بأفضل شكل عن طريق تحديد الأهداف بوضوح منذ البداية وبمساندة مؤسسات تعاونية. يساعد هذا التعاون على تجنب بناء إنترانت خاصة بمجموعة معينة من الموظفين. حيث أن معرفة ماهية المستخدمين قبل البدء بالتخطيط يضمن بأن تكون الإنترانت ذات قيمة جيدة من حيث المضمون، وسهلة الاستخدام بالنسبة لجميع المستخدمين.

وعلى الرغم من أن الإنترانت لا تأخذ الشكل ذاته بنظر جميع المستخدمين، فإن فهم قدرات ونقاط ضعف مستخدمي الإنترانت يضمن بناء إنترانت ذات قيمة عامة.

لا يمكن أن توجد شبكتا إنترانت متشابهتان، لكن شبكات الإنترانت الناجحة تتشارك بخصائص أساسية، والمفاتيح الأساسية لنجاح الإنترانت هي:

- وضوح الرؤية.
- تحديد الأهداف.
- تحديد توقعات واقعية.
- تعريف نموذج متعدد الاختصاصات.
- ضمان تدخل المستخدم.
- استمرار المتابعة.

الفصل الثاني

الشبكات المحلية

بعد أن استعرضنا مفاهيم الإنترانت وأهميتها في الفصل الأول سنقوم في هذا الفصل والفصول القادمة بتفصيل بنية شبكة الإنترانت والمتطلبات الأساسية لبنائها.

في البداية لا بدّ من توضيح البنية المادية التحتية لأي شبكة إنترانت وهي شبكات الاتصالات المحلية (Local Area Networks <LAN>)، وهذا الفصل يعرض البنية المادية لهذه الشبكات وكذلك المفاهيم الأساسية الواجب فهمها للمتابعة في باقي الفصول.

إن أبسط شكل لشبكة اتصالات محلية هو وصل حاسوبين أو أكثر بهدف تمكين الحواسيب الموصولة بالشبكة من التخاطب بعضها مع بعض من جهة والتشارك على موارد الشبكة من جهة أخرى. وتُستخدم الشبكات المحلية في المؤسسات الحكومية والمدارس والجامعات وشركات الأعمال الخاصة وذلك لتأمين الاستثمار الأمثل للموارد المتاحة من قبل المشتركين في الشبكة، إضافةً إلى تأمين الاتصال فيما بينهم.

ولكن عملية بناء شبكة اتصالات محلية في بيئة ما هي عملية حساسة ومعقدة نوعاً ما ؛ إذ يجب البدء بدراسة المتطلبات الأساسية لهذا المحيط قبل الخوض في تفاصيل بناء الشبكة، ففي البداية يجب تحديد نظام تشغيل الشبكة ونوعية أسلاك التوصيل ومن ثم مناقشة نوعية الخدمات الواجب

تقديمها للمستخدمين وكيفية حصول المستخدمين على هذه الخدمات، وفي أي وقت تجب إتاحة هذه الخدمات، ....

على سبيل المثال، إذا أردنا تزويد الشبكة بطابعات، فتجب مواجهة العديد من الأسئلة لاختيار عدد الطابعات المطلوبة: ما هو عدد المستخدمين في الشبكة ؟ كم هو عدد الطابعات الضروري لتلبية حاجات هؤلاء المستخدمين ؟ هل يوجد مستخدم معين يحتاج إلى طابعة شخصية غير قابلة للتشارك مع مستخدم آخر لضمان وثوقية ما ؟ ....

وهكذا نجد أنه يجب تحديد المتطلبات أولاً، ومن ثم التكنولوجيا التي تلبي هذه المتطلبات، كي نستطيع أن نبدأ في إعداد الشبكة المحلية، وعندها يمكن أن نجد العديد من الخيارات التي تستطيع تلبية الحاجات المختلفة.

إن دراسة أنواع الشبكات المحلية الموجودة حالياً والأخرى المتوقعة في المستقبل ضرورية لاختيار الشبكة المحلية المثلى التي ستعمل عليها الإنترانت المراد تصميمها.

يوضح هذا الفصل طرق وصل الحواسب والشبكات، وكذلك البنى الفيزيائية والبرمجيات المتعددة المتاحة لتكوين شبكة اتصالات محلية، إضافةً إلى الخدمات التي يمكن أن تقدمها هذه الشبكات وكيفية الاستفادة منها.

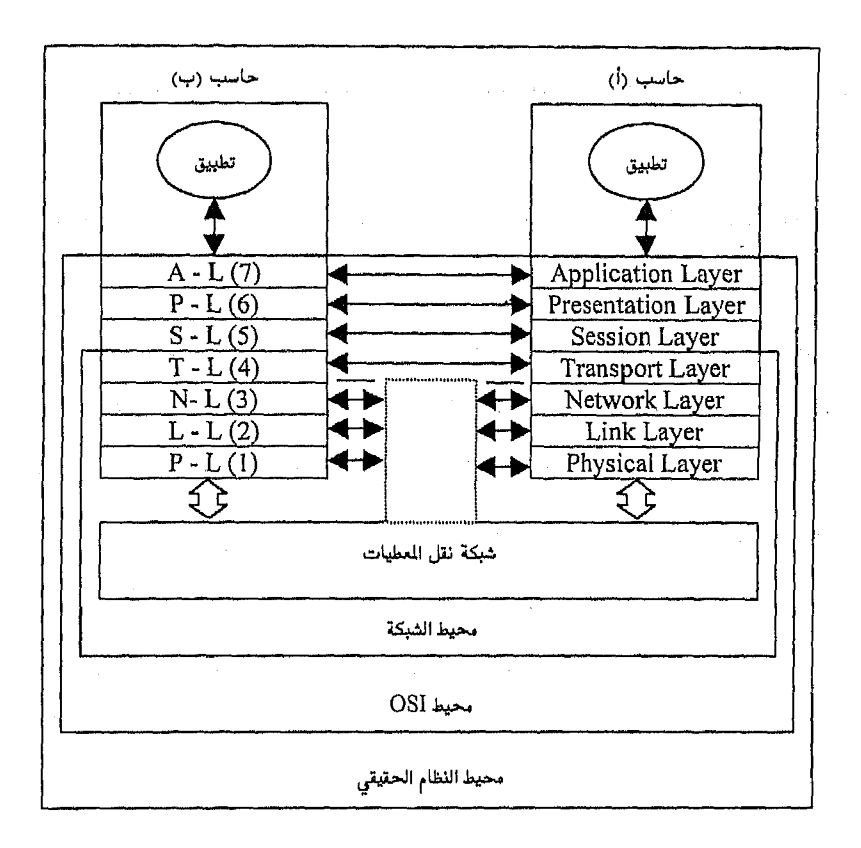
2-1 النموذج ISO/OSI للشبكات المحلية

تبنت منظمة المعايير العالمية ISO (International Standards Organization) نموذجاً معيارياً طبقياً لتوصيف بنية أي شبكة اتصال، حيث قُسِّمت بنية الشبكة إلى عدة طبقات (Layers) لكل منها وظيفته المحددة. يمكن النظر إلى هذه الطبقات على أنها تقوم بإحدى وظيفتين: وظائف متعلقة بالشبكة، ووظائف خاصة بالتطبيقات، وهذا أدى بدوره إلى تمييز ثلاثة أقسام رئيسية تختلف في

اعتمادها على تبادل المعلومات المتعلقة ببنية الشبكة أو بطبيعة الخدمات أو بالمستخدم النهائي. وهذه الأقسام هي:

- *محيط الشبكة:* ويتعلق بالمعايير والبروتوكولات الخاصة بمختلف أنماط نقل المعطيات في الشبكة.
- *محيط ربط النظم المفتوحة OSI (Open System Interconnection):* يُغلّف المحيط السابق مع إضافة المعايير والبروتوكولات الخاصة بالتطبيقات التي تسمح لنقاط الشبكة النهائية (الحواسيب) بالاتصال فيما بينها بطريقة مفتوحة عبر المحيط السابق.
- *محيط النظام الحقيقي:* يُغلّف هذا المحيط محيط OSI ويحتوي على البرمجيات والخدمات الخاصة بالمصنّعين والتي صُممت للقيام بمهمات خاصة لمعالجة المعطيات الموزّعة.

يوضّح الشكل (2–1) النموذج ISO/OSI لبنية الشبكات المحلية:



الشكل (2-1): نموذج ISO/OSI المعياري

يبين الشكل السابق أن محيط OSI يُقسم إلى عدة طبقات متسلسلة لكل منها وظيفتها الخاصة (فيزيائية كانت أم برمجية).

تشكل الطبقات السبع المبينة في الشكل البناء الأساسي لأي شبكة اتصال، أما المحيط الثالث فهو معني بالمستخدم النهائي فقط ولا يُناقش عند دراسة بنية الشبكة.

تهتم الطبقات الثلاث الأولى (1-3) من نموذج OSI ـ بمساعدة البروتوكولات المترافقة معها ـ بعملية نقل المعلومات وتبادلها عبر الشبكة، وتُسمى هذه الطبقات الثلاث بالطبقات المرتبطة بالشبكة (Network Dependent Layers). بينما تهتم الطبقات الثلاث الأخيرة (5-7) بالسماح لإجرائيات

المستخدم النهائي بالاتصال بعضها مع بعض وتُسمى بالطبقات المستقلة عن الشبكة (Network Independent Layers).

أما الطبقة الرابعة (طبقة النقل) فهي تلعب دوراً وسيطاً، إذ تحجب عن الطبقات المستقلة عن الشبكة الوظائف الروتينية للطبقات المرتبطة بالشبكة كما تؤمن الاتصال بينهما.

ولكل من هذه الطبقات السبع الوظيفة الخدمية الخاصة بها، وسنقوم بعرض هذه الوظائف فيما يلي.

2-1-1 الطبقة الفيزيائية

تشمل الطبقة الفيزيائية (Physical Layer) الوسط الفيزيائي لنقل المعطيات، وواجهات الربط الإلكترونية وهي تؤمن وصل تجهيزات المستخدم إلى الشبكة، كما تقدم للطبقة التي تليها (طبقة الوصل) المعطيات المنقولة ما بين محطتين متخاطبتين.

2-1-2 طبقة الوصل

تُبنى طبقة الوصل (Link Layer) على الوصلات الفيزيائية، وهي مسؤولة عن معالجة أخطاء النقل وإعادة الإرسال في حالة وجود الأخطاء، وتقسم هذه الطبقة إلى طبقتين فرعيتين هما:

- MAC (Media Access Control).
- LLC (Logical Link Control).

2-1-3 طبقة الشبكة

تُعتبر طبقة الشبكة (Network Layer) مسؤولة عن العنونة والتوجيه وتقسيم المعطيات الكبيرة الحجم القادمة من الطبقة الأعلى إلى كتل محددة الطول في حالة الإرسال، والتأكد من استلام هذه الكتل كاملة وتجميعها ثم إرسالها إلى الطبقة الأعلى في حالة الاستقبال.

2-1-4 طبقة النقل

تُنظّم طبقة النقل (Transport Layer) تدفق المعطيات وتعطي لكل رسالة رقماً معيناً لضمان وصول الرسائل وفق ترتيب إرسالها، كما تقوم بعملية مزج العديد من الرسائل لإرسالها عبر قناة اتصال واحدة.

2-1-5 طبقة جلسة الاتصال

تُعتبر طبقة جلسة الاتصال (Session Layer) مسؤولة عن إدارة الحوار أثناء الاتصال، حيث يقوم المستخدم النهائي بالاتصال مع هذه الطبقة مباشرة للتعبير عن رغبته في إقامة جلسة اتصال مع الجهة الأخرى عبر الشبكة، وتقوم هذه الطبقة بالتحكم بزمن الاتصال وعبور المعطيات، والاهتمام بتصحيح أخطاء النظام.

2-1-6 طبقة العرض

تهتم طبقة العرض (Presentation Layer) بموضوع عرض المعطيات المنقولة في محطات الشبكة، وتلعب دور المترجم بين المحطات، كما أنها تؤدي بعض الوظائف المتعلقة بأمن الشبكة.

2-1-7 طبقة التطبيقات

تُنظّم طبقة التطبيقات (Application Layer) اتصال المستخدم النهائي عبر الشبكة حيث أنها تحتوي نظام تشغيل الشبكة والتطبيقات التي تعمل مع هذا النظام، وهذه الطبقة لا يحكمها بروتوكول محدد لأنها تعتمد على طرق عمل التطبيقات التي تحتويها، كالبريد الإلكتروني وقواعد البيانات المشتركة وغيرها.

بقي أن نذكر أن النموذج OSI/ISO ليس النموذج المعياري الوحيد في تمثيل بنية الشبكات، فهناك نماذج أخرى مثل النموذج CCITT، ولكننا استعرضنا OSI/ISO لأنه الوحيد المتبع في بناء الشبكات المحلية.

2-2 المكونات الفيزيائية

عند دراسة تصميم أي شبكة محلية تأتي دراسة الكيان الفيزيائي لها في المرتبة الأولى، على اعتبار أن الهدف الأساسي هو وصل عدة حواسيب بعضها ببعض بواسطة الأسلاك لتشكيل مكونات الشبكة المحلية الأولية. وقد يظن البعض أن المكونات الفيزيائية للشبكة تعني الطبقة الفيزيائية الواردة في نموذج ISO/OSI ولكن هذه المكونات قد تشمل فعلياً أكثر من طبقة في هذا النموذج، فأغلب الشبكات المحلية متشابهة من حيث البنية ويمكننا عند دراسة الكيان الفيزيائي لها أن نغطي الطبقة الفيزيائية وطبقة الوصل معاً، حيث أنه يمكن لكيان فيزيائي محدد أن يؤدي وظائف الطبقتين معاً باستخدام برتوكول وحيد.

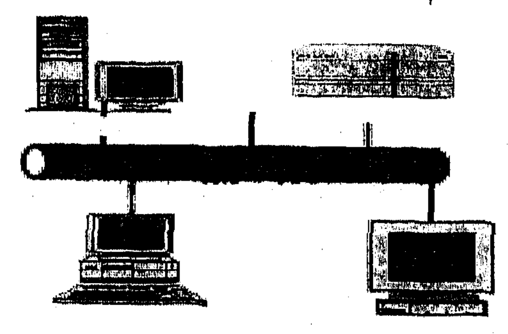
ولتحديد ماهية هذا البروتوكول لا بد أولاً من تصميم الشبكة المحلية فيزيائياً وذلك بتحديد خصائص وسط نقل المعطيات الذي سيربط حواسيب الشبكة فيما بينها، وتحديد طريقة ربط هذه الحواسيب، إضافةً إلى تحديد خصائص منفذ المعطيات من وسط النقل إلى الحواسيب.

2-2-1 طبولوجيا الشبكات المحلية

تتميز معظم الشبكات المحلية بأنها محصورة في مساحة جغرافية ضيقة نسبياً مما يعني أن المسافات الفاصلة بين الحواسيب المطلوب ربطها إلى الشبكة غالباً ما تكون محدودة، الأمر الذي يبسط كثيراً عملية بناء طبولوجيا الشبكة، والمقصود بمصطلح طبولوجيا الشبكة هو الشكل الذي تأخذه الحواسيب والوصلات فيما بينها عند تشكيل الشبكة المحلية، ويمكن تصنيفها إلى:

آ- طبولوجيا المر المشترك (Bus Topology)

تعتمد هذه الطبولوجيا على خط نقل وحيد يؤمن وصل جميع حواسيب الشبكة بعضها ببعض (الشكل 2-2)، وهذه الطبولوجيا سهلة التحقيق عملياً وغير مكلفة ولكنها غير فعّالة أمام الأعطال، فقد يؤدي عطل واحد في خط النقل إلى فصل معظم الحواسيب عن الشبكة.



الشكل (2-2): طبولوجيا المر المشترك

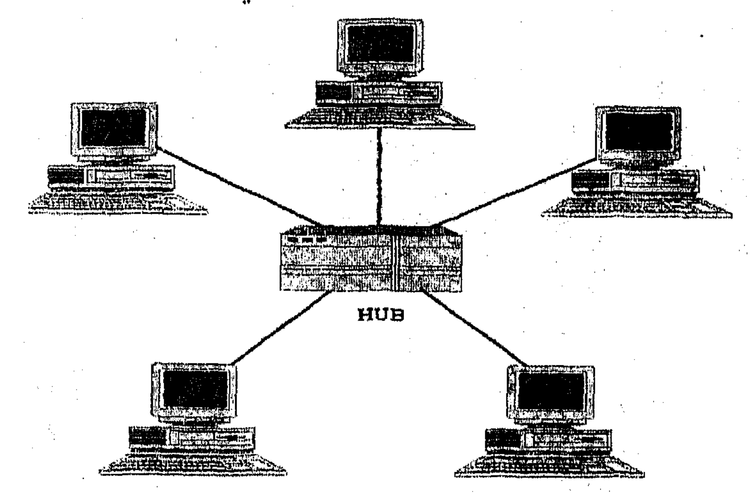
ب- طبولوجيا النجمة (Star Topology)

تُوصل الحواسيب في هذه الحالة عن طريق مُجمِّع (Hub)، حيث يُوصل كل حاسوب إلى المجمع بواسطة خط نقل، وتتم عملية التخاطب بين حاسوبين على الشبكة من خلال المجمع، وبذلك تأخذ الشبكة شكل نجمة (الشكل 2-3) ومن هنا أتت التسمية، وتتميز هذه الطبولوجيا بأن حاسوباً واحداً فقط ينفصل عن الشبكة في حال حدوث عطل ما في خط نقل.

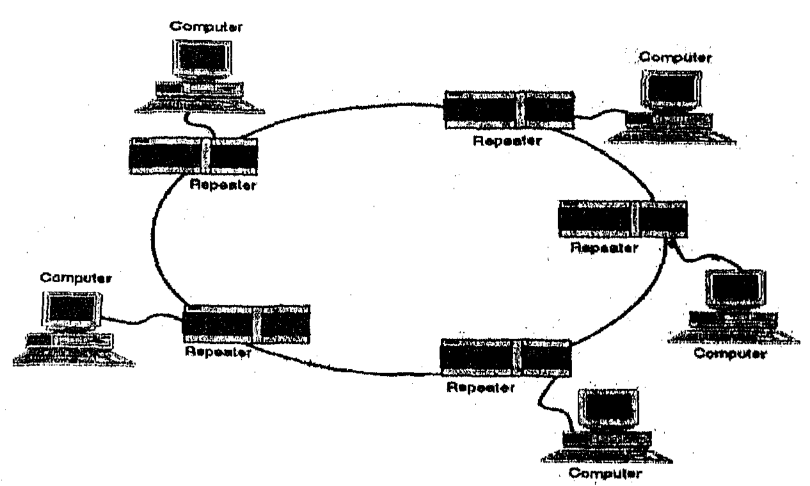
ج- طبولوجيا الحلقة (Ring Topology)

تُربط الحواسيب في هذه الحالة على شكل حلقة بواسطة خطوط النقل، وبالتالي فإن كل حاسوب سيرتبط مع حاسوبين مجاورين له (الشكل 2-4). وتتميز هذه الطبولوجيا بتقنية الوصل المعروفة باسم

"نقطة إلى نقطة" (Point to Point) بين كل حاسوب والحاسوبين المجاورين له، ولكي يتخاطب حاسوب ما وحاسوب بعيد يجب المرور بالعديد من الحواسيب الأخرى، وبالتالي عند حدوث عطل ما في أحد خطوط النقل تفقد الشبكة معظم إمكانيات التخاطب بين محطاتها المتباعدة بعضها عن بعض، ولكنها تحافظ على التخاطب نقطة إلى نقطة المحقق بين باقي المحطات غير المتضررة من العطل.



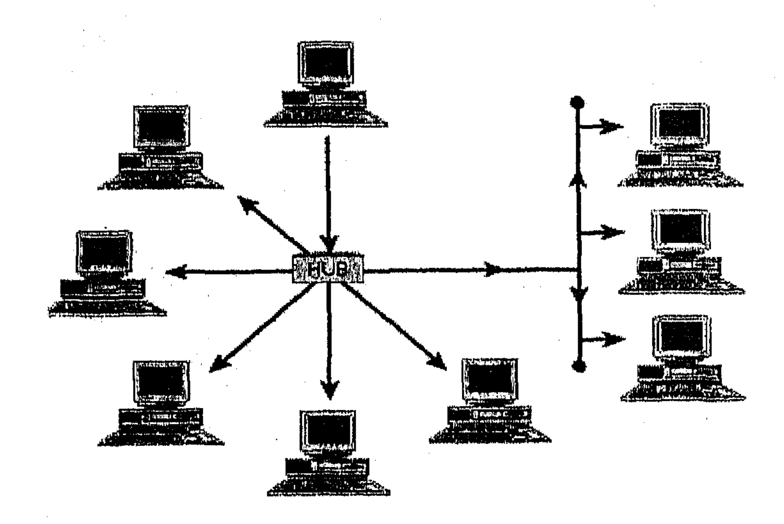
الشكل (2-3): طبولوجيا النجمة



الشكل (2-4): طبولوجيا الحلقة

د- طبولوجيا المجمع (Hub Topology)

هذه الطبولوجيا هي مزيج من طبولوجيا الخط وطبولوجيا الحلقة، حيث تُربط عدة شبكات تستخدم طبولوجيا الخط لتشكيل حلقة باستخدام مجمع لربط خطين متجاورين (الشكل 2-5)، وبذلك يتخاطب أي حاسوبين واقعين على خط واحد وفق طبولوجيا الخط، وأي حاسوبين في خطين متجاورين عبر المجمع، وأي حاسوبين متباعدين عن طريق المرور بأكثر من مجمع.



الشكل (2-5): طبولوجيا المجمع

2-2-2 وسائط النقل في الشبكات المحلية

سنستعرض في هذه الفقرة وسائط النقل المستخدمة في ربط الحواسيب فيما بينها لتكوين الشبكة المحلية. حيث يمكن تمييز أربعة أنواع من الوسائط المستخدمة في ربط الحواسيب في أيّ شبكة محلية حالية، وهذه الوسائط هي:

- الأسلاك المحورية Coaxial.

- الثنائيات المجدولة Twisted Pair.
- الألياف الضوئية Optic Fiber.
- الوصل اللاسلكي Wireless.

تنتقل المعطيات بين حواسيب الشبكة المحلية عبر إحدى وسائط النقل السابقة والتي تختلف درجة ملاءمتها للشبكة باختلاف خصائصها، كسرعة النقل والوثوقية وغيرها من الخصائص المميزة المعروضة في الفقرات القادمة.

من الجدير بالذكر أنه يمكن استخدام أكثر من وسيطة نقل واحدة في وصل الشبكة المحلية كاستخدام الألياف الضوئية في بعض أجزاء الشبكة واستخدام الأسلاك المحورية (Coaxial) في أجزاء أخرى، وفي هذه الحالة لا بد من وجود جهاز يؤمن تحويل الإشارة المنقولة في الألياف الضوئية إلى ما يوافقها في الأسلاك المحورية في نقطة الوصل، وفيما يلي دراسة تفصيلية لخصائص هذه الأوساط الناقلة.

آ- الأسلاك المحورية (Coaxial Cables)

استخدمت هذه الأسلاك في الجيل الأول من شبكات الاتصالات المحلية لوصل الحواسيب فيما بينها. ويتألف السلك المحوري من سلكٍ مركزي يدعى الناقل ويكون من النحاس عادة، ويُغلّف بعازل بلاستيكي وتلتف حول العازل شبكة معدنية رقيقة من الأسلاك مغطاةً بغطاء بلاستيكي.

تمر إشارة المعطيات عبر الشبكة المحلية في الناقل المركزي، أما الشبكة المعدنية المحيطية فتعمل كأرضي للإشارة، وأبسط مثال لاستخدامات هذا النوع من أوساط النقل هو نقل الإشارة التلفزيونية.

تكمن أهمية هذه الأسلاك في دورها في حماية الإشارة المنقولة عبر الناقل المركزي من التداخل مع إشارات المنابع الإلكترونية الخارجية (أي الإشعاع الإلكتروني الناتج عن أي منبع مجاور آخر مثل الضوء أو المكيف) وهو الدور الذي تقوم به شبكة الأسلاك المعدنية المحيطية.

أما سلبيات هذا النوع من الأسلاك فهي حساسيتها الشديدة للثني، مما يؤدي إلى تشويه الإشارة. وعلى الرغم من استبدال الثنائيات المجدولة بهذا النوع من الأسلاك في العديد من الشبكات، فإن بعض الشبكات المحلية لا تزال تستخدمه.

ب- الثنائيات المجدولة (Twisted Pair)

تتألف الثنائيات المجدولة من زوج من الأسلاك الملفوفة بعضها حول بعض والمغلفة بغلاف خارجي عازل، تُستخدم هذه الأسلاك في وصل الشبكات الهاتفية إلى المنازل، وذلك لسهولة تصنيعها وعدم حساسيتها للثني مقارنةً مع الأسلاك المحورية، ولكنها بالمقابل ذات معدل نقل أقل بسبب تأثرها بالتداخل مع إشارات النواقل الأخرى المجاورة.

صُمّمت أنواع مختلفة من الأغلفة العازلة للثنائيات المجدولة وأصبحت تصنّف حسب تسلسل عازليتها، وقد جرى التوصل إلى درجة عالية من العازلية بحيث أصبح بإمكان الثنائيات المجدولة منافسة الأسلاك المحورية وحتى التفوق عليها.

ويمكن القول عموماً أنّ استخدام الثنائيات المجدولة ذات العازلية الكبيرة يسمح بالحصول على شبكة محلية ذات سرعة عالية.



الشكل (2-6): الثنائيات المجدولة

ج- الألياف الضوئية (Optic Fiber)

أحدث دخول الألياف الضوئية في عالم الاتصالات كوسيطة نقل ثورةً هائلة بالنسبة لسرعة نقل المعطيات، وتُعتبر حتى الآن وسيطة النقل المثلى تقنياً، ولا يمكن لأي وسيطة نقل أخرى منافستها إلا من الناحية الاقتصادية حيث أنها ما تزال مكلفة نوعاً ما.

يتكون الليف الضوئي من جزأين رئيسيين هما اللب والقشرة ؛ يُصنع اللب من مادة زجاجية مرنة رفيعة جداً يكون قطرها بحدود 125 µm ، أما القشرة فهي مادة بلاستيكية لحماية الليف. تنتقل الإشارة في الألياف الضوئية عبر اللب ، وتكون هذه الإشارة ضوئية بدلاً من أن تكون كهربائية كما في حالة الأسلاك المحورية والثنائيات المجدولة ، وهذا بدوره كفيل بحل مشكلة التداخل الناتجة أساساً عن استخدام الإشارات الكهربائية ، حيث أن الإشارات الضوئية يمكن أن تعمل في وسط مليء بالضجيج الكهربائي دون أن تتأثر بذلك مما يزيد من معدّل النقل.

كما تتميز الألياف الضوئية بمردود نقل أعظمي عند نقلها للإشارات الرقمية ، وهذا ما يجعلها الوسيطة الأكثر وثوقية بين الوسائط المستخدمة في وصل الشبكات.

يتم تمثيل الواحد المنطقي في الألياف الضوئية بمرور ضوء ، والصفر بعدم مرور ضوء ، بينما يجري تمثيل هاتين الحالتين كهربائياً في حالة الأسلاك المحورية أو الثنائيات المجدولة ("5" فولت من أجل الواحد المنطقي ، و"-5" فولت من أجل الصفر المنطقي).

وعلى الرغم من الميزات الإيجابية الكثيرة للألياف الضوئية ، إلا أن سلبياتها تحد من كثرة استخدامها محلياً حتى الوقت الحاضر ، وذلك بسبب كلفتها العالية نسبياً وصعوبة تركيبها (في المباني مثلاً) وصعوبة توافقها مع الأسلاك الأخرى.

د- الوصل اللاسلكي (Wireless)

عند وصل الشبكة المحلية لاسلكياً فإن الحواسيب الموصولة تستخدم مستقبلات ومرسلات الترددات الراديوية RF (Radio Frequency) بدلاً من استخدام الأسلاك ، ومن ثم يكون وسط النقل في هذه الحالة هو الفضاء ، ويقوم كل حاسوب بإرسال واستقبال المعطيات من وإلى الحواسيب الأخرى مستخدماً البث بالأمواج الكهرطيسية الراديوية بالطريقة نفسها التي تعمل بها أجهزة الراديو.

قد يبدو للبعض أن هذه الطريقة هي الأسهل والأفضل لوصل الحواسيب في شبكة محلية ولكن هناك بالطبع العديد من النقاط التي تمس أمن الشبكة المحلية ووثوقية النقل فيها على وجه الخصوص، ويجب أن تؤخذ بعين الاعتبار.

النقطة الأولى التي تمس أمن الشبكة هي إرسال حواسيب الشبكة للمعطيات عبر الفضاء وبالتالي فإن هذه المعطيات ستكون مكشوفةً لكل من يهمه استقبالها وليس فقط للجهة المستقبلة، الأمر الذي يتطلب تشفير المعطيات قبل إرسالها في حالة الحاجة إلى السرية العالية مما يعقّد الموضوع أكثر مما يجب، حيث أن عملية تشفير المعطيات خاضعة لاحتمال فك التشفير وهذا يعني وجوب إيجاد نظام تشفير عالي الوثوقية، وهو أمر مكلف إلى حد ما وغير مرغوب فيه إذا كان محيط الشبكة العملية قابلاً للتغطية سلكياً.

النقطة الثانية والمهمة من الناحية الأمنية هي احتمال حدوث اختراق غير مرغوب به من خارج الشبكة، ولا يمكن معالجة هذه النقطة عملياً إلا باتخاذ إجراءات أمنية عالية تعالج موضوع النفاذ غير المشروع إلى الشبكة، ويمكن ذكر العديد من الحوادث المشابهة في نظام الهاتف الخليوي، حيث أنه بمجرد معرفة رمز النفاذ إلى هاتف خليوي ما يمكن استخدامه ووضع آلاف الدولارات عليه، ونظام الاتصالات في الشبكة المحلية اللاسلكية، شأنه شأن نظام الهاتف الخليوي، يستخدم إشارات RF، ومن غير الممكن إحصاء عدد القادرين على التنصت على نظامٍ يستخدم إشارات RF.

النقطة الأخيرة هي وثوقية الشبكة المحلية اللاسلكية حيث أن الفضاء المستخدم كوسط نقل للأمواج الراديوية مزدحم بعدد لا يحصى من الإشارات الراديوية التي من شأنها إنقاص وثوقية الشبكة ورفع معدل خطأ نقل المعطيات وهذه النقطة لا تقل أهمية عن أمن الشبكة.

توضح النقاط السابقة التناقض بين مفهوم أمن الشبكة والوصل اللاسلكي، حيث أنه من المفضل استخدام الوصل السلكي كلما كان ذلك ممكناً وذلك في المساحات المحدودة، كما أنه من الممكن الوصل باستخدام الألياف البصرية في المساحات الواسعة، فعلى سبيل المثال يمكن وصل حواسيب في

أمريكا الشمالية بحواسيب في أوروبا باستخدام جسر الألياف البصرية الممتد بين القارتين وذلك لتشكيل شبكة محلية (في حال شركة ذات فروع متعددة مثلاً)، مع الحفاظ على أمن الشبكة.

تتحدّد تقنية الوصل الواجب استخدامها في شبكة محلية باختيار إحدى التقنيات الأربع المذكورة سابقاً، ويتحدد هذا الاختيار تبعاً لعدة عوامل كالعوامل الجغرافية، ونوعية نظام تشغيل الشبكة المعتمد، ومتطلبات معدل الإرسال، وأخيراً أمور الصيانة.

ومن الواضح حالياً أن الألياف البصرية تسرق الأضواء شيئاً فشيئاً، ومن المرجّح أن تصبح في المستقبل إحدى الميزات العامة في الشبكات المحلية، فتكاليفها تنخفض تدريجياً مع الزمن وسوف تحل محل طرق التوصيل الأخرى. ولكن في الوقت الحالي فإن كلاً من التقنيات الأربع السابقة الذكر لها ميزاتها في وصل الشبكات المحلية ويجب مناقشتها تباعاً عند الشروع في تصميم أي شبكة محلية.

2-2-3 واجهات ربط الشبكات المحلية

تُعتبر واجهات ربط الشبكات المحلية (LAN Interfaces) العنصر المكمّل لعمل وسيطة النقل في الشبكة المحلية، حيث أنها تمثل نواة الوصل الفعلي بين وسيطة نقل المعطيات والحواسيب. وعند الحديث عن تصميم البنية المادية للشبكة المحلية يجب اعتبار وسيطة النقل الواجب استخدامها للربط بين حواسيب الشبكة، إضافةً إلى واجهة الربط المطلوبة لتأمين اتصال وسيطة النقل مع كل حاسوب من حواسيب الشبكة.

يُربَط الحاسوب (أو أي عتاد آخر) عادةً بالشبكة المحلية فعلياً باستخدام بطاقة واجهة ربط الشبكة (Network Interface Card <NIC>)، وتسمى هذه البطاقة أحياناً بطاقة التحكم بالنفاذ إلى الوسيطة (Media Access Control <MAC>). تُثبت هذه البطاقة في الحاسوب على نحوٍ مشابه لتثبيت أي بطاقة أخرى (مثل بطاقة التحكم بالأقراص المضغوطة مثلاً، أو بطاقة الصوت، ...). كما أنه من الممكن أن تكون هذه البطاقة مسبقة التثبيت في بعض الحواسيب، وتشكل بطاقات الربط واجهة التعامل مع الشبكة وتقوم بدور الطبقة الثانية (طبقة الوصل) في النموذج ISO/OSI.

يجري تبادل المعطيات في المستوى الفيزيائي باستخدام عنوان فيزيائي لكل محطة أو طرفية ويتعلق هذا العنوان بنمط الشبكة. يُعطى العنوان عند التصنيع بطريقة ثابتة ووحيدة، أما بالنسبة للتطبيقات فإنها تتخاطب على نحو مستقل عن نمط الشبكة (إذ يمكن وجود شبكة تتضمن عدة شبكات فرعية من أنماط مختلفة) وذلك باستخدام عنوان منطقي مثل العنوان IP (أو عنوان الإنترنت). ولتحقيق التقابل بين العنوانين الفيزيائي والمنطقي هناك بروتوكولات خاصة (البروتوكول ARP/RARP من عائلة البروتوكولات TCP/IP).

لتأمين تخاطب الحاسوب عبر الشبكة المحلية تقوم بطاقة الشبكة بأداء وظيفتين أساسيتين وهما النفاذ إلى الشبكة وتهيئة المعطيات عند الإرسال والاستقبال.

آ- النفاذ إلى الشبكة

تتميز كل بطاقة شبكة محلية بخوارزمية خاصة بها (تُسمى بروتوكولاً) تؤمن لأي حاسوب النفاذ إلى الشبكة وإجراء الاتصال المرغوب به عبر الشبكة، وتختلف هذه الخوارزمية من شبكة إلى أخرى باختلاف بطاقة واجهة الربط المعتمدة في كل شبكة.

يقدّم الحاسوب طلب الاتصال إلى بطاقة الشبكة الموجودة فيه فتقوم البطاقة بدورها بإجراء الخوارزميات المعتمدة لتأمين نفاذ هذا الحاسوب إلى الشبكة، وفي الحالة العكسية تقوم بطاقة الشبكة أيضاً باستقبال طلب خارجي من الشبكة لإشراك الحاسوب في الاتصال المطلوب.

يوجد العديد من البروتوكولات المعتمدة للنفاذ إلى الشبكة وسوف نقوم بدراستها بالتفصيل عند استعراض الأنواع المختلفة من بطاقات الشبكة المحلية المستخدمة حالياً.

ب- تهيئة المعطيات عند الاستقبال والإرسال

تنقل المعطيات عبر خط النقل على شكل إطارات (Frames)، والإطار هو سلسلة محدّدة من الخانات الثنائية (Bits) ويكون محدّداً بخانة بداية وخانة نهاية ويحمل المعلومات بين بدايته ونهايته،

ويعتمد شكل الإطار المنقول على نوعية البروتوكول المستخدم في الشبكة، ويتعلق هذا البروتوكول بنوع بطاقة واجهة ربط الشبكة التي تؤدي وظائف كل من الطبقة الفيزيائية وطبقة النقل.

تقوم بطاقة الشبكة عند الإرسال باستلام المعطيات من الطبقات الأعلى في الحاسوب على شكل كتل معطيات تسمى الطرود (Packets)، وقبل إرسالها عبر خط النقل تضيف إليها معطيات خاصة بالبروتوكول المعتمد فيها لتشكيل الإطار القابل للإرسال عبر خط النقل، والذي تستقبله إحدى بطاقات الشبكة المشابهة في طرف الاستقبال، وتكون البطاقة المستقبلة قادرة على فهم محتويات الإطار لأنها تستخدم نفس البروتوكول.

من ثم نجد أن بطاقة الشبكة غير معنية بمضمون الطرود المرسلة والمستقبلة بين الحواسيب، بل تتعامل معها كصناديق سوداء، وتضيف إليها معطيات خاصة بها (مثل عنوان المرسل، عنوان المستقبل، نظام معالجة الأخطاء) وذلك لتشكيل إطار الإرسال.

تقوم بطاقة الشبكة في حالة الاستقبال بتجريد هذا الإطار من الحشو المضاف إليه والخاص بالبروتوكول المعتمد فيها، وتسلّم طرود المعطيات إلى الطبقة الأعلى في الحاسوب المستقبل بحيث تكون هذه الطرود مطابقة لتلك التي وردت من البطاقة المرسِلة.

توجد عدة أنواع من بطاقات الشبكة المحلية المستخدمة حالياً وتتميز هذه البطاقات بكونها بطاقات معيارية (Standard) تستخدم بروتوكولات تحكم معيارية، وتتميز بعضها عن بعض من حيث سرعة النقل والوظائف الأساسية التي تقوم بها (تهيئة المعطيات، والنفاذ إلى الشبكة)، وطبولوجيا الشبكة المستخدمة.

البطاقة إثرنت Ethernet 802-3

تُعتبر بطاقة إثرنت (أو البطاقة 802-3) أكثر البطاقات استخداماً كواجهة ربط في الشبكات المحلية، وكانت شركة DEC أول من قام بتصميمها، ومن ثم عُدّلت من قبل معهد مهندسي الكهرباء والإلكترونيات الأمريكي IEEE، واعتبرت كمعيار عالمي تحت اسم IEEE 802-3.

تعتبر هذه البطاقة من البطاقات السريعة في نقل المعطيات، حيث تستطيع إرسال 10 مليون خانة ثنائية خلال ثانية واحدة عبر خط شبكة محلية، وتدعى أحياناً ببطاقة الـ 10 MBps وذلك نسبةً لمعدل إرسالها (Baud Rate)، وقد جرى مؤخراً إصدار نسخة أسرع من هذه البطاقة يصل معدل إرسالها إلى 100Mbps وذلك لدعم التطبيقات التي تحتاج إلى هذه السرعة الفائقة في نقل المعطيات.

تقوم بطاقة إثرنت بتهيئة إطار الإرسال كما يلي:

يرسل هذا الإطار عبر خط النقل وتكون كل الإطارات المنقولة ذات طول ثابت، وكما يبين الشكل (2-7) فإن الإطار يحوي الحقول التالية:

- *حقل محدد البداية (Start Delimiter)*: يستخدم هذا الحقل كمقدمة بهدف ضبط التزامن بين المرسل والمستقبل.
- *الحقل SFD*: يؤشر هذا الحقل على بداية إطار قابل للاستقبال ويتبع المقدمة مباشرة وهو بطول ثُمانية (بايت Byte) واحدة.

الحقل	الطول
محدد البداية	7 بايت
SFD	1 بايت
عنوان المرسل	2 أو 6 بايت
عنوان المستقبل	2 أو 6 بايت
مؤشر الطول	2 بايت
المعطيات	أقل من 1518 بايت
التحقق من صحة المعلومات	4 بايت

الشكل (2-7): إطار إثرنت

- *حقول عنوان المرسل وعنوان المستقبل (Source and Destination Address)*: يحمل هذان الحقلان عنوان المرسل وعنوان المستقبل، وكل منهما بطول 16 أو 48 خانة ثنائية، ويجب تحديد أحد الطولين في شبكة محلية معينة. تحدّد الخانة الأولى من عنوان المستقبل فيما إذا كان العنوان هو عنوان شخصي أو عنوان مجموعة، فإذا كان عنواناً شخصياً فسيجري استقباله من قبل محطة عمل وحيدة (حاسوب وحيد)، أما إذا كان عنوان مجموعة فإن عدة محطات سوف تستقبل هذا الإطار. وفي الحالة الخاصة التي يكون فيها عنوان المستقبل يحوي "1" في كل خاناته فإن الإطار سوف يُعمّم على كل المحطات العاملة على الشبكة.
- *حقل مؤشر الطول (Length Indicator)*: يؤشر هذا الحقل على الطول الفعلي للمعلومات، ويستخدم لتوحيد طول الإطار المنقول على خط النقل، إذ إن بطاقة إثرنت تضيف إلى المعطيات الفعلية بعض المعطيات الإضافية لتوحيد الطول.
- *حقل التحقق من المعلومات (Frame Check Sequence)*: يستخدم هذا الحقل لكشف الأخطاء التي قد تحدث أثناء النقل.

عند استقبال الإطار تستخلص بطاقة الإثرنت المعطيات المفيدة منه وتعالج الأخطاء إن وردت ومن ثم ترسل المعطيات المفيدة إلى الطبقة الأعلى في الحاسوب المستقبل.

تعتمد شبكة إثرنت بروتوكول النفاذ المتعدد بتحسس الحامل/فحص التضارب (Carrier Sensing Multiple Access/ Collision Detection <CSMA/CD>) الذي يعتمد على مبدأ وجود مستخدم وحيد قادر على النفاذ إلى الشبكة في لحظة ما، ولحل مشكلة التصادم تقوم بطاقة إثرنت بفحص خط الشبكة لتحديد انشغاله أو خلوه من المستخدمين، فعندما تكون لدى الحاسوب معطيات للإرسال يقوم نظام CSMA/CD بفحص الخط للتأكد من عدم وجود عملية إرسال جارية على الخط، فإذا كان ذلك محققاً فإن الحاسوب يستلم الخط لإرسال المعطيات، وفي حالة انشغال الخط ينتظر الحاسوب فترة معينة ثم يعاود الفحص مرة ثانية، ولا يستطيع الإرسال حتى خلو الخط.

قد يحدث أن يطلب حاسوبان الخط في نفس الوقت، عندها يجري تمرير إنذار تضارب عبر الشبكة إلى كل الحواسيب فتنتظر كل حواسيب الشبكة فترة وجيزة (جزء من الثانية) قبل معاودة طلب الخط للإرسال. تحتّم الخوارزمية المتبعة في النفاذ إلى الشبكة المحلية عبر بطاقة إثرنت على كل مستخدم يريد التخاطب عبر الشبكة المحلية الانتظار حتى خلو الخط. ومن الجدير بالذكر أن شبكة إثرنت تستخدم طبولوجيا الخط أو طبولوجيا النجمة، حيث يستخدم خط محوري في حالة استخدام طبولوجيا الخط، وتستخدم الثنائيات المجدولة في حالة استخدام طبولوجيا النجمة، والحالة الأخيرة هي الأكثر شيوعاً في شبكات إثرنت.

بطاقة تمرير السماحية الحلقية (Token Ring)

قامت شركة IBM بنشر هذه البطاقة أولاً، ومن ثم استخدمتها في بيئاتها الخاصة (شبكة حواسيب Mainframe)، إلى أن قام المعهد الأمريكي IEEE بإيجاد معيار موافق لهذه البطاقة أُدرج تحت الاسم 802.5 ؛ ولهذه البطاقة نمطان أساسيان لا يختلفان إلا بسرعة نقل المعطيات وهما: النمط 4MBps والنمط 16MBps.

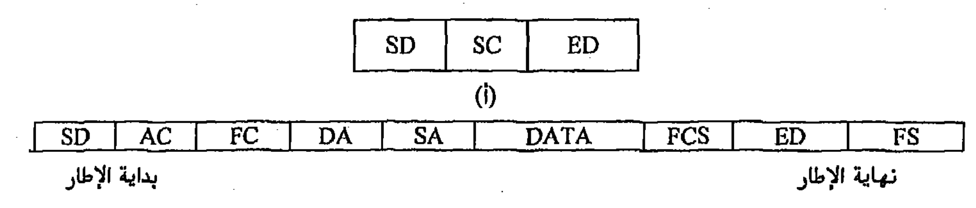
تدير شبكة Token Ring الحوار عبر الشبكة (خوارزمية النفاذ إلى الشبكة) باستخدام "Token" إلكترونية تعبّر عن السماحية المتاحة للمحطة بالنفاذ إلى الشبكة. تُسمى هذه السماحية بـ "حق الحوار" في هذه الحالة، وهي تنتقل من محطة إلى أخرى وفق ترتيب حلقي محدّد ومعروف لكل المحطات المربوطة على الشبكة، حيث يقوم الحاسوب المالك للسماحية بإرسال إطار واحد فقط عبر خط النقل ومن ثم يمرر السماحية إلى الحاسوب التالي (حسب ترتيب أولوية السماحيات) ليملك هذا الأخير حق الإرسال عبر خط النقل ؛ ويمكن تلخيص ما سبق بالخطوات التالية:

- يجري بناء حلقة منطقية تمر بكل المحطات عبر الشبكة المربوطة إلى خطوط النقل، وتبنى سماحية منطقية واحدة.

- تمر السماحية عبر الحلقة المنطقية إلى كل محطات الشبكة إلى أن يستقبلها أحد الحواسيب المنتظرة لإرسال إطار من المعطيات.
- يرسل الحاسوب الذي يملك حق الحوار الإطار المنتظر إلى خطوط النقل ومن ثم تُمرر السماحية إلى المحطة التالية في الحلقة المنطقية.

تقوم بطاقة Token Ring بتهيئة نوعين من الإطارات، فبالإضافة إلى تهيئة إطار المعلومات للإرسال عبر خطوط الشبكة تقوم البطاقة بتهيئة إطار السماحية الإلكترونية.

يوضح الشكل (2-8) السماحية والإطار بعد التهيئة:



الشكل (2-8): شكل الإطار (ب) والسماحية (آ) في شبكة Token Ring

وبالنسبة للحقول المستخدمة في الشكل لدينا:

- *حقل محدد البداية (Start Delimiter) SD*: يحدد بداية الإطار أو السماحية.
- *حقل محدد النهاية (End Delimiter) ED*: يحدد نهاية الإطار أو السماحية.
- *حقل التحكم بالنفاذ (Access Control) AC*: يُعتبر هذا الحقل مسؤولاً عن تحديد الأولوية وله الشكل التالي:

P	P	P	T	M	R	R	R

حيث تُعبّر الخانات الثنائية P عن الأولوية، وتُعبّر الخانات الثنائية R عن السماحية للمحطات التي لديها إطارات ذات أولوية عالية بالحصول على الأولوية، أما الخانة الثنائية

T فهي للتمييز بين السماحية (T = 0) والإطار (T = 1)، في حين تـدل الخانـة الثنائيـة M على المرسل الحالي.

- *حقل حالة الإطار FS (Frame Status):* يعبر هـذا الحقـل عـن حالـة الإطـار ولـه الشـكل التالي:

A	C	X	X	A	C	X	X

حيث تكون كلٌ من الخانتين الثنائيتين A و C صفـراً في المحطـة المرسـلة، ويقـوم المسـتقبل صاحب العنوان DA عند استقبال الإطار بوضع "1" في الخانة A، وعنـد نسخ الإطار يقـوم بوضع "1" في الخانة C، وذلك ليتأكد المرسل إن كان العنوان المقصود فعّال علـى الشـبكة أم لا، وإذا كان فعّالاً، إن كان قد قام بنسخ الإطار أم لم يقم بذلك.

تطابق الحقول FCS, DATA, DA, SA تماماً الحقول الموافقة لها في شبكة إثرنـت، غـير أن طول المعلومات DATA قد يختلف بين الشبكتين.

أخيراً، إن شبكة Token Ring غير مضطرة لاستخدام الطبولوجيـا الحلقيـة وذلـك لأن حلقـة انتقـال السماحية بالنفاذ هي حلقة منطقية وليس من الضروري أن تكون الشبكة حلقيةً فيزيائياً لبنـاء الحلقـة المنطقية، ومن ثم فـإن شـبكة Token Ring قـد تسـتخدم الطبولوجيـا النجميـة، وفي كلتـا الحـالتين تُستخدم الثنائيات المجدولة كوسيطة للنقل.

بطاقة Token Bus

طوِّرت هذه البطاقة مـن قبـل شـركة DataPoint الأمريكيـة في السـبعينات، وهـي تعتـبر مزيجـاً مـن البطاقتين السابقتين، وقد اعتمدت من قبل المعهد الأمريكي IEEE وأصدرت البطاقـة 802.4 كتقييـس عالمي لهذه البطاقة.

تنقل بطاقة Token Bus المعطيات بسرعة 2.5MBps، وتُعتبر هذه السرعة محدودة أمام أنواع البطاقات الأخرى، مما يجعل الشبكات المحلية التي تستخدم هذه البطاقة قليلة الانتشار ولا تتعدى الشبكات المنزلية والمصانع.

ولتجنب التكرار لن نخوض في شرح بنية الإطار وبروتوكول النفاذ إلى الشبكة المحلية Token Bus وذلك للتشابه الكبير بينها وبين تلك المستخدمة في شبكة Token Ring، ولكن الفرق الجوهري بينهما يكمن في سرعة نقل المعطيات ومواضع الاستخدام وطبولوجيا الشبكة، حيث أن شبكة Token Bus تستخدم طبولوجيا الخط.

بطاقة FDDI

تعتبر بطاقة المعطيات الموزعة بواسطة الألياف الضوئية (Fiber Distributed Data Interface <FDDI>) من البطاقات ذات السرعة العالية في نقل المعطيات (100MBps). تستخدم هذه البطاقة تقنية النفاذ بتمرير السماحية (Token Passing) وطبولوجيا حلقية مزدوجة ؛ حيث تستخدم شبكة FDDI زوجاً من الألياف الضوئية لوصل كل محطة، وهذه الثنائية في الوصل تؤمن عدم انقطاع اتصال أي محطة مع الشبكة المحلية عند حدوث عطل مفاجئ في إحدى الوصلات. يوضح الشكل (2-9) طريقتي وصل الشبكة المحلية FDDI، حيث من الممكن تمييز نوعين من محطات الشبكة:

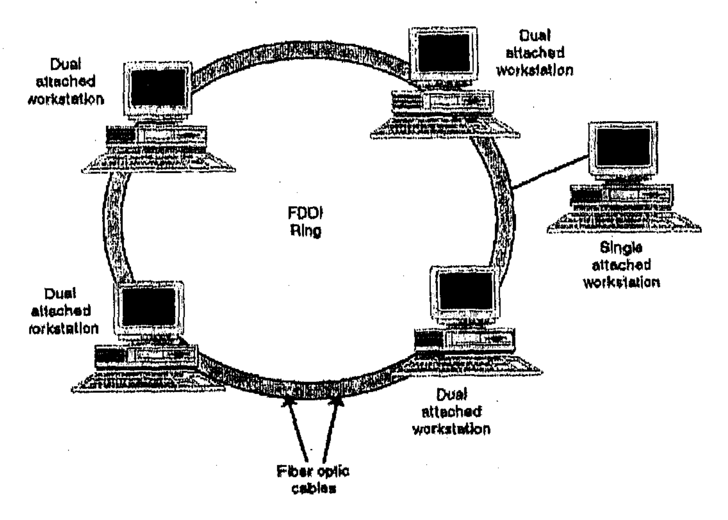
- المحطات ثنائية الوصل DAS (Dual Attached Stations).
- المحطات أحادية الوصل SAS (Single Attached Stations).

تتميز الشبكة المحلية FDDI باستخدامها للألياف الضوئية كوسيطة نقل، مما يعني الوثوقية العالية لهذه الشبكة وعدم وجود مشاكل أمنية، مما يجعلها الخيار الأول عند تصميم شبكة محلية في بيئة عمل تتطلب السرية والوثوقية (المؤسسات الحكومية والتجارية).

وبسبب التكلفة العالية للألياف الضوئية وصعوبة وصلها في كل مكان فقد تضطر شبكة FDDI إلى التخلي عن استخدام الألياف الضوئية في الوصل على مستوى الحواسيب والاكتفاء بها على مستوى

المباني مثلاً، حيث تستخدم الثنائيات المجدولة لإتمام عملية الوصل إلى الحواسيب بعد استخدام محوّل خاص يحول إشارة الليف الضوئي إلى إشارة كهربائية متوافقة مع الثنائيات المجدولة، وكذلك تجري عملية التحويل المعاكس طبعاً.

ومن الجدير بالذكر أنه يمكن بناء الشبكة المحلية FDDI باستخدام الثنائيات المجدولة فقط، وعندها تسمى هذه الشبكة باسم البطاقة CDDI، أو بطاقة المعطيات الموزعة بواسطة النحاس (Copper Distributed Data Interface <CDDI>).



الشكل (2-9) شبكة FDDI

بطاقة ATM

ما تزال بطاقة نمط النقل غير المتزامن ATM (Asynchronous Transfer Mode) غير معتمدة رسمياً لأن التقنية المستخدمة في بنائها مازالت قيد التطوير والبحث، وما يزال النموذج المعياري لها قيد التعريف.

تعتمد هذه البطاقة كسابقتها على الألياف الضوئية كوسيطة نقل في الشبكة، وتبدأ سرعة النقل فيها من 150 وتصل إلى 600MBps، وتعتمد شبكة ATM على تقنية النقل بواسطة التبديل الخليوي

(Cell-Switching Transport) حيث تقوم بضغط المعطيات المنقولة في مجموعات صغيرة ذات حجم ثابت، مما يسمح بالوصول إلى سرعات نقل هائلة جداً عند استخدام الألياف الضوئية كوسيطة نقل.

ورغم التكلفة العالية لشبكة ATM إلا أنها وضعت قيد الخدمة وجرى تصميم وبناء عدة شبكات محلية باستخدام البطاقة ATM من قبل بعض الشركات الكبرى وعلى رأسها شركة IBM، وتجري الآن عمليات تعريف المعيار العالمي لهذه البطاقة حيث أنها تعتبر البطاقة المثلى لبيئات الشبكات المحلية التي تتطلب خدماتها سرعاتٍ نقل متزايدة.

تبقى بطاقة ATM غير قابلة للاستخدام من قبل الشركات العادية التي، حتى وإن استطاعت دفع التكاليف الهائلة لبناء الشبكة المحلية ATM بسرعة نقل 155MBps للحصول على خدمات عالية المستوى مثل نقل الملفات هائلة الحجم ونقل الصور والفيديو مثلاً، فإن هذه الشركة ستعاني من مشكلة اختناق في الشبكة عند وصلها مع خط هاتفي بسرعة نقل 1.54MBps، وسوف يكون استخدام البطاقة ATM مجرد هدر مالي.

بعد استعراض التقنيات المستخدمة في بناء الشبكة المحلية يبقى على المصمم البحث لاختيار إحدى هذه التقنيات لبناء البنية التحتية للإنترانت المطلوبة، وذلك بالمقارنة بين نوعية الخدمات التي تقدمها كل بنية فيزيائية وتكاليف تحقيق هذه البنية.

3-2 البروتوكولات TCP/IP

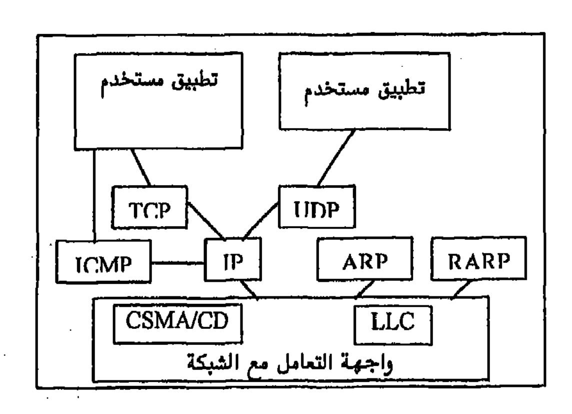
بدأ استخدام هذه البروتوكولات في الولايات المتحدة الأمريكية عام 1969 من قبل وزارة الدفاع الأمريكية DoD (Department of Defense) حيث استخدمت لأول مرة في شبكة محلية تخص هذه الوزارة، كما استخدمت في بناء شبكة الإنترنت وباتت تسمى "لغة الإنترنت"، غير أنها مستخدمة الآن على نحوٍ شائع في بناء الشبكات المحلية سواء وُصلت مع شبكة الإنترنت أم لم توصل.

يقوم البروتوكول TCP/IP بمهام طبقة الشبكة وطبقة النقل، وهو في الواقع اجتماع بروتوكولين: الأول هو البروتوكول IP (Internet Protocol) الذي يغطي طبقة الشبكة ويعتبر كوسيط بين طبقة الوصل وطبقة النقل، والثاني هو البروتوكول TCP (Transmission Control Protocol) ويغطي طبقة النقل ولا يستطيع تأدية وظائفه ما لم يتعامل مع البروتوكول IP تحديداً في طبقة الشبكة، ولذلك سنتعامل مع هذين البروتوكولين تحت اسم واحد هو البروتوكول TCP/IP.

يتميز البروتوكول TCP/IP بأنه ملائم لكافة أنواع الشبكات المحلية المدروسة (شبكة إثرنت، Token Ring، Token Bus، FDDI، وشبكة ATM)، وبالتالي يمكن بناؤه فوق أي بروتوكول مكوّن للطبقتين الأوليتين في نموذج ISO/OSI.

وفي شبكات الإنترانت وشبكة الإنترنت فإن بروتوكولات TCP/IP تعمل مع مجموعة من البروتوكولات المعيارية لتقديم خدمات هذه الشبكات، وهذه البرتوكولات تُسمى أحياناً عائلةَ بروتوكولات TCP/IP أو مجموعة بروتوكولات TCP/IP. يوضّح الشكل (2-10) بروتوكولات العائلة TCP/IP وما يقابلها في طبقات النموذج ISO/OSI.

7	طبقة التطبيقات
6	طبقة العرض
5	طبقة الجلسة
4	طبقة النقل
3	طبقة الشبكة
2	طبقة الوصل
1	الطبقة الفيزيائية



الشكل (2-10): بروتوكولات العائلة TCP/IP

وفيما يلي سنقوم بتفصيل أهم هذه البروتوكولات التي ستذكر في عدة مواضع من الكتاب.

2-3-1 البروتوكول IP

يقوم البروتوكول IP بأداء معظم وظائف طبقة الشبكة، وأهم هذه الوظائف هي عمليات تقسيم المعطيات وتوجيهها، حيث يقوم البروتوكول IP بتقسيم المعطيات الواردة من الطبقات الأعلى إلى طرود تدعى طرود IP، وتكون هذه الطرود من وجهة نظر هذا البروتوكول مستقلة بعضها عن بعض بعد عملية التقسيم، بحيث يجري تسليمها واحداً تلو الآخر إلى الطبقة الأدنى (طبقة الوصل) لتكون نواةً يجري تغليفها لتشكيل إطارات الإرسال. وبالطبع فإن البروتوكول IP يقوم بإعادة تجميع هذه الطرود عند استقبالها من الطبقات الدنيا لتجميع المعطيات الأصلية ونقلها إلى الطبقات الأعلى.

وبالرغم من كون البروتوكول IP مسؤولاً عن تحديد المسار الذي ستسلكه المعطيات لبلوغ وجهتها النهائية (وظيفة التوجيه)، إلاّ أنه غير مسؤول عن التأكد من الاستقبال السليم لهذه المعطيات من قبل المستقبل، كما أنه غير مسؤول عن التحكم بتدفق المعطيات، إذ أن هذه الوظائف تعتبر من وظائف الطبقة الأعلى (طبقة النقل أو البروتوكول TCP).

يُعتبر طرد IP توصيفاً كاملاً لعمل البروتوكول IP، حيث يجري تشكيل الطرد بعد عملية تقسيم المعطيات، إذ يضيف البروتوكول IP إلى المعطيات المنقولة عبر الشبكة حقولاً للتحكم تسبق المعطيات المفيدة وهذه الحقول تدعى ترويسة (Header) الإطار IP. يُوضح الشكل (2-11) هذه الترويسة:

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td colspan="4">رقم النسخة</td><td colspan="4">طول المقدمة</td><td colspan="8">نمط الخدمة</td></tr>
<tr><td colspan="16">الطول الكلي</td></tr>
<tr><td colspan="16">التعريف</td></tr>
<tr><td></td><td>D
F</td><td>M
U</td><td colspan="13">الإزاحة</td></tr>
<tr><td colspan="8">مدة الحياة</td><td colspan="8">البروتوكول</td></tr>
<tr><td colspan="16">اختبار الترويسة</td></tr>
<tr><td colspan="16">عنوان المرسل</td></tr>
</table>

عنوان المستقبل
الخيارات — حشو
المعطيات (≥ 65536 بايت)

حقل نمط الخدمة:

9	10	11	12	13	14	15	16
حقل الأولوية			D	T	R	Unused	

الشكل (2-11): ترويسة الإطار IP

- *حقل النسخة (Version Field):* يتضمن هذا الحقل رقم نسخة البروتوكول IP.

- *حقل طول المقدمة IHL (Internet Header Length):* يحوي هذا الحقل طول المقدمة مقدّراً بعدد الكلمات (طول كل كلمة 32 خانة ثنائية)، حيث أن كل الحقول في ترويسة الطرد ذات طول ثابت ومعتمد في كل الطرود، ماعدا حقل الخيارات.

- *حقل نمط الخدمة (Type of service):* يضم هذا الحقل 8 خانات ثنائية موزعة على خمسة أقسام وفق الشكل التالي:

1- قسم الأولوية (Priority): يُعطى لكل طرد رقم يعبر عن أولويته، يتراوح هذا الرقم بين 0 (أولوية عادية) و 7 (أولوية الإشراف على الشبكة Supervision). نميّز الطرودَ استناداً على رقم الأولوية لتحديد أهمية تسهيل سيرها عبر الشبكة، فعلى سبيل المثال تعطى أولوية عالية لمعلومات التحكم.

2- الخانة الثنائية D: تطلب الإسراع في إيصال الطرد إذا كانت تحمل القيمة واحد.

3- الخانة الثنائية T: تطلب التدفق العالي للمعطيات إذا كانت تحمل القيمة واحد.

4- الخانة الثنائية R: تطلب الوثوقية العالية إذا كانت تحمل القيمة واحد.

5- خانات ثنائية غير مستخدمة.

وتستخدم الخانات الأخيرة من قبل خوارزميات التوجيه عند إمكانية وجود أكثر من طريق للوصول إلى الطرف المستقبل، ويتم تحقيق طلبات هذه الخانات قدر الإمكان.

- *حقل الطول الكلي (Total length)*: يتضمن هذا الحقل عدد الثمانيات الكلية المكونة للطرد (والمقدمة مع حقل المعلومات)، وبما أن طول هذا الحقل 16 خانة ثنائية فنستطيع إذن ترميز 2^{16} رقماً، وبذلك يبلغ الطول الكلي الأعظمي المسموح للرزمة 65635 خانة ثنائية.

ومن الجدير بالذكر أن الطول الكلي الأعظمي للطرد يتعلق بالطول الأعظمي للإطار الفيزيائي (الذي سوف يغلف هذه الرزمة في الطبقات الأدنى والذي سينتقل عبر الشبكة) المسموح به في الشبكة المحلية، ويسمى هذا الطول (للإطار) وحدة النقل الأعظمية (Maximum Transfer Unit <MTU>)، وتختلف MTU من شبكة إلى أخرى باختلاف واجهة الربط الشبكية المستخدمة، وعند ربط شبكات مختلفة من حيث MTU يقوم البروتوكول IP بتجزئة الطرد إلى أجزاء أصغر (Fragments) عند عبورها من شبكة إلى أخرى عبر المعابر (Gateways)، بحيث يكون طول الجزء منها مساوياً لوحدة النقل الأعظمية MTU للشبكة المرسل إليها، والتي ستعامل كلاً من هذه الأجزاء كطرد IP خاص بها، وفي الحالة العكسية تقوم الشبكة المستقبلة بتجميع هذه الأجزاء وتكوّن طرد IP الأصلي. يجري التحكم بعملية التجزئة والتجميع السابقة عن طريق الحقول الأربعة التالية.

- *حقل التعريف (Identification)*: يحتوي هذا الحقل على رقم يميز أجزاء الطرد الواحد، إذ يجب على جميع أجزاء الطرد الواحد المجزئ أن تحمل هذا الرقم.

- *خانة عدم التجزيء DF (Don't Fragment)*: تطلب هذه الخانة عندما تأخذ القيمة 1 عدم تجزئة الطرد IP من قبل البوابات، وعند ذلك يُمرر هذا الطرد كاملاً في الطريق الذي يسمح بنقله كاملاً دون تجزئة، وإلاّ فإنه يلغى.

- *خانة زيادة التجزئة* *MF (More Fragment)*: عندما يُجزأ الطرد IP توضع هذه الخانة على القيمة 1 في جميع أجزاء الطرد الناتج (الطرود الجزئية) ما عدا الجزء الأخير حيث توضع على الصفر. وبالاعتماد على هذه الخانة وحقل الطول الكلي نستطيع معرفة إن كانت الأجزاء قد وصلت كاملةً أم لا.
- *حقل الإزاحة (Fragment Offset)*: يدل هذا الحقل على مقدار انزياح أول ثمانية يتضمنها الجزء عن بداية الطرد الأصلية وذلك باعتبار وحدة القياس 8 ثمانيات، وعندها يجب أن يكون طول كل الأجزاء ما عدا الجزء الأخير من مضاعفات 8 ثمانيات.
- *حقل مدة الحياة (Time To Live)*: يعبر هذا الحقل عن المدة الأعظمية مُقاسةً بالثواني لحياة الطرد IP المسموح بها عبر الشبكة المحلية، وتوضع في هذا الحقل قيمة ابتدائية تبدأ بالتناقص في كل عقدة تعالج الطرد بمقدار بقائه في هذه العقدة، وعند وصول هذه القيمة إلى الصفر يُلغى الطرد بهدف منع تجواله عبر الشبكة إلى ما لا نهاية. طول هذا الحقل 8 ثمانيات مما يسمح بمدة حياة أعظمية تبلغ 255 ثانية.
- *حقل البروتوكول (Protocol)*: يحدد هذا الحقل نوع بروتوكول الطبقة الأعلى (طبقة النقل) المسؤول عن استلام المعطيات وتسليمها للبروتوكول IP كبروتوكول TCP أو غيره من البروتوكولات.
- *حقل اختبار الترويسة (Header Checksum)*: يسمح هذا الحقل بالتحقق من صحة القيم الواردة في حقل التحكم في الطرد.
- *حقول عنوان المرسل وعنوان المستقبل* *SA & DA (Source and Destination Address)*: يحدد هذان الحقلان عنوان الطرف المرسل والطرف المستقبل في الشبكة المحلية، ويسمى هذا العنوان بعنوان الإنترنت أو بعنوان IP (Internet or IP Address). يبلغ طول كل حقل 32 خانة ثنائية، ويتألف من عنوان الشبكة المحلية إضافةً إلى عنوان الحاسوب في الشبكة.

- *حقل الخيارات (Options):* وهو حقل اختياري بطول غير محدد يحوي بعض المتحولات التي قد تطلبها الجهة المرسلة.
- *حقل الحشو (Padding):* يستخدم هذا الحقل من أجل تتميم المقدمة إلى مضاعفات 32 من حيث الطول، ويجري هذا التتميم بإضافة مجموعة من الأصفار.

وهكذا نجد أن البروتوكول IP ينجز وظائف طبقة الشبكة بالاعتماد على خصائص العنونة التي يتميز بها، مما يسمح بتوجيه جيدٍ للرسائل عبر الشبكة المحلية نفسها، أو حتى عبر الشبكات الأخرى المتصلة بها، مما يجعله البرتوكول الوحيد المستخدم في شبكات إنترانت التي تتميز بإمكانية تخاطبها مع شبكة الإنترنت.

2-3-2 البروتوكول TCP

يقوم بروتوكول التحكم بالنقل TCP (Transmission Control Protocol) بمهام طبقة النقل في الشبكات المحلية، حيث يقوم بتأمين اتصال موثوق بين طرفي الاتصال وذلك بالتحقق من وصول الطرود المرسلة إلى المستقبل باستخدام خوارزمية تعتمد إشارة الإقرار (Acknowledgment) بوصول الطرد، والتي يقوم الطرف المستقبل بإرسالها للطرف المرسل. ويقوم البروتوكول TCP بترقيم الطرود المتبادلة أثناء عملية التخاطب لتمييز إشارات الإقرار بوصول الطرود، حيث تحمل كل إشارة إقرار رقم الطرد مما يعني وصوله بسلامة، ويقوم البروتوكول TCP بعملية إعادة إرسال الطرود المفقودة التي لم تصل إشارة إقرار بوصولها من قبل الطرف المستقبل. وباعتماد الخوارزمية السابقة يستطيع الطرف المستقبل المحافظة على الترتيب الصحيح للطرود ويضمن عدم فقدان بعضها عبر الشبكة، مما يؤمن وثوقية عالية في عملية تبادل الرسائل.

كما يقوم البروتوكول TCP بالتحكم بتدفق المعطيات عبر الشبكة باستخدام مبدأ النافذة المنزلقة (Sliding Window)، الأمر الذي يحقق التوافق في سرعة نقل المعطيات بين الطرف المرسل والطرف

المستقبل. يعتمد هذا المبدأ على نافذة متغيرة الطول وذات طول أعظمي يحدد العدد الأعظمـي للطـرود المسموح بإرسالها دون ورود إشارات إقرار بوصولها، فعندما يبدأ الطرف المرسل بإرسال الطرود يكـون طول النافذة المنزلقة معدوماً، ويزداد بمقدار واحدٍ عند إرسال كل طرد وينقص بالمقدار نفسه عند ورود إقرار بوصول طرد، وعندما يصل طول هذه النافذة إلى حدّه الأعظمي يتوقف المرسل عن عملية الإرسال منتظراً إشارات الإقرار بالطرود المرسلة وذلك خلال فـترة زمنيـة محـددة مسـبقاً، فـإذا لم تـرد إشـارة الإقرار بوصول الطرد الأول (كما هو مرتب في النافذة) خلال هذه الفترة يقوم المرسل بإعـادة الإرسـال. وباعتماد مبدأ النافذة المنزلقة يقوم البروتوكول TCP بترقيم الطرود وفقاً للطول الأعظمي لهذه النافذة.

يتعامل البروتوكول TCP مباشرةً مع طبقة التطبيقات في الطبقة الأعلى وفق نموذج ISO/OSI، ويؤمن عملية المزج (Multiplexing) بين تطبيقات عديدة يمكن أن تقـوم بعمليـة التخـاطب عـبر الشـبكة في الوقت نفسه. وتجري عملية نقل المعطيات من كل تطبيق يجري تخاطباً عـبر الشـبكة إلى الـبروتوكول TCP عبر منفذ للمعطيات يفتح بين طبقة التطبيقات وطبقة النقل ويدعى هذا المنفذ بالبوابـة (Port)، حيث تملك كل بوابة عاملة رقماً يميزها ويعتبر بمثابة عنـوان لهـا ممـا يمكّـن الـبروتوكول TCP مـن تمييز التطبيقات المختلفة في محطة العمل التي تتخاطب عبر الشبكة. أما على مسـتوى الشـبكة ككـل فيجري تمييز كل اتصال بواسطة رقم البوابة المميز للتطبيق الذي يسـتخدم طبقـة النقـل بالإضافـة إلى العنوان IP الذي يميز نقطة الوصول إلى بروتوكولات طبقات الشبكة الدنيـا، وذلـك في كـلٍ مـن طـرفي الاتصال. وتشكل الثنائية (رقم البوابة، العنوان IP) ما يُسمى بالمقبس (Socket) الذي يميز كل اتصال عبر الشبكة بصورة وحيدة.

يقوم البروتوكول TCP باستلام المعطيات من التطبيق عـبر البوابـة ثـم يقـوم ببنـاء الرزمـة TCP الـتي تتضمن المعطيات الأصلية إضافةً إلى الترويسة TCP، ويوضح الشكل (2–12) البنية التفصيلية للرزمـة TCP.

32 خانة ثنائية

<table dir="rtl">
<tr><td colspan="2">عنوان البوابة المستقبلة</td><td colspan="3">عنوان البوابة المرسلة</td></tr>
<tr><td colspan="5">الرقم التسلسلي</td></tr>
<tr><td colspan="5">رقم الإقرار</td></tr>
<tr><td colspan="2">نافذة</td><td>FLAGS</td><td>خانات محجوزة</td><td></td></tr>
<tr><td colspan="2">مؤشر الطوارئ</td><td colspan="3">اختبار الصحة</td></tr>
<tr><td>حشو</td><td colspan="4">خيارات</td></tr>
<tr><td colspan="5">المعطيات</td></tr>
</table>

الشكل (2-12): شكل رسالة TCP

تتضمن الرزمة TCP حقول التحكم التالية:

- *حقل البوابة المرسلة (Source Port)*: يحدد هذا الحقل عنوان (رقم) البوابة المحددة من قبل التطبيق المرسل في الحاسوب المرسل.
- *حقل البوابة المستقبلة (Destination Port)*: يحدد هذا الحقل عنوان (رقم) البوابة المحددة من قبل التطبيق المستقبل في الحاسوب الوجهة. ومن الواضح أن هناك إمكانية لعنونة 2^{16} بوابة (إرسال أو استقبال) في كل محطة عمل.
- *حقل الرقم التسلسلي (Sequence Number)* يحدد هذا الحقل الرقم التسلسلي الذي يعطيه البروتوكول TCP للرزمة المرسلة.
- *حقل إشارة الإقرار (Acknowledgment Number)*: يحدد هذا الحقل رقم الرزمة التي ينتظر المرسل إقراراً بوصولها من المستقبل، ويعتبر هذا الرقم إقراراً من المرسل على وصول جميع الإقرارات بوصول الرزم ذات الأرقام السابقة، وفي هذه الحالة يمكن للمستقبل أن يعيد إرسال الإقرارات التي لم تصل للمرسل في حال ضياعها عبر الشبكة. يتألف هذا الحقل من 32 خانة ثنائية.

- *حقل انزياح المعطيات (Data Offset):* يحدد هذا الحقل تسلسل الثمانية الأولى في هذه الرزمة بالنسبة لبداية الرسالة، ويتألف هذا الحقل من 4 خانات ثنائية.
- *حقل المؤشرات (Flags):* ويتألف هذا الحقل من 6 خانات ثنائية للتحكم وهي:
  - URG: وتدل على وجود معلومات طارئة للإرسال عندما تأخذ القيمة واحد.
  - ACK: وتدل على أن حقل رقم الإقرار السابق يؤدي وظيفته المذكورة عندما تأخذ القيمة واحد أو أنه بلا معنى عندما تأخذ القيمة صفر.
  - PSH: وتدل في لحظة معينة على أن كل الرزم المرسلة قد وصلت إلى المستقبل عندما تأخذ القيمة واحد.
  - RST: وتدل على إعادة تهيئة الاتصال (Reset) عندما تأخذ القيمة واحد.
  - SYN: وتدل على التزامن في الترقيم منذ البدء بعملية الاتصال.
  - FIN: وتدل على نهاية الاتصال الجاري عندما تأخذ القيمة واحد.
- *حقل النافذة (Window):* يحدد هذا الحقل حجم النافذة المنزلقة المستخدمة في الاتصال، ويتألف من 16 خانة ثنائية.
- *حقل الاختبار (Checksum):* يسمح هذا الحقل بالتحقق من صحة القيم الواردة في حقول التحكم في هذه الرزمة، ويبلغ طوله 16 خانة ثنائية.
- *حقل مؤشر الطوارئ (Urgent Pointer):* يعمل هذا الحقل بالتوافق مع الخانة URG في حقل المؤشرات، فإذا دعت الحاجة إلى إرسال أمر مفاجئ عبر الشبكة إلى الطرف المستقبل، وكان هذا الأمر يتطلب معالجة فورية، فيمكن إرسال هذا الأمر (بعد قطع إرسال الرسالة الحالية) وتجري الإشارة إلى موقع هذا الأمر في حقل المعطيات بواسطة هذا المؤشر.

- *حقل الخيارات (Options):* وهو حقل اختياري بطول غير محدد يحوي بعض التحولات التي قد تطلبها الجهة المرسلة.
- *حقل الحشو (Padding):* يستخدم هذا الحقل من أجل تتميم المقدمة إلى مضاعفات 32 من حيث الطول، ويجري هذا التتميم بواسطة مجموعة من الأصفار.

أخيراً، يمكن اعتبار البروتوكول TCP المسؤول عن عملية فتح قناة الاتصال بين التطبيق المرسل والتطبيق المستقبل، حيث يقوم التطبيق المرسل بإرسال طلب إجراء تخاطب مرسلاً للبروتوكول TCP عنوان المقبس الوجهة، حيث يؤمن هذا البروتوكول الاتصال المطلوب بالوثوقية المطلوبة بالتعاون مع البروتوكولات الأدنى في طبقات الشبكة الأدنى.

2-3-3 البروتوكول UDP

وهو بروتوكول نقل يسمح بإرسال واستقبال معطيات بين البرامج التطبيقية، ويمكن مقارنة الخدمة المقدمة من UDP بخدمة البريد، فهو لا يحتاج إلى إقامة مسبقة للاتصال (نمط Connectionless) كما أنه لا يؤمن وثوقية النقل (أي لا يصحح الأخطاء، ولا يضمن تسلسل المعطيات، ...). يعتبر UDP المعطيات المرسلة سلسلة من الرسائل، ويضيف عليها ترويسته الخاصة ويمررها إلى بروتوكول النقل IP، ويُظهر الشكل (2-13) بنية هذه المقدمة.

31 … 23	15 … 7
عنوان البوابة المستقبلة	عنوان البوابة المرسلة
التحق من الأخطاء	الطول
// المعطيات	

الشكل (2-13): شكل رسالة UDP

2-4 نظم تشغيل الشبكة

يُعتبر نظام تشغيل الشبكة NOS (Network Operating System) الموجه والقائد لكل موارد الشبكة المحلية، فهو يؤدي في الشبكة الوظيفة نفسها التي يؤديها نظام تشغيل الأقراص (Disk Operating System <DOS>) في الحاسوب من حيث تعريف الموارد الأساسية، وكيفية استثمار هذه الموارد استثماراً أمثلياً، ولكن نظام تشغيل الشبكة يقوم بهذه الوظيفة من أجل كل حاسوب مربوط إلى الشبكة ومن أجل موارد الشبكة ككل، فهو المسؤول عن تنظيم عملية النفاذ إلى مورد مشترك بين عدة مستخدمين، وعن عملية تنظيم الملفات القابلة للتشارك بين محطات الشبكة، وعن تخزين هذه الملفات وفق خوارزمية معينة تجعل تشارك المستخدمين فيها أمراً سهلاً.

وبشكل آخر يمكن القول إن نظام تشغيل الشبكة هو المسؤول عن إدارة الخدمات التي تقدمها الشبكات المحلية للمستخدمين، وقد تختلف طبيعة هذه الخدمات باختلاف الشبكة المحلية (المجلدات المشتركة، الطابعات المشتركة،...)، مما يؤدي إلى اختلاف نظام التشغيل المعتمد في الشبكات المحلية من شبكة إلى أخرى بما يتوافق مع الخدمات المتاحة من قبل الشبكة المحلية. وبالمقابل يوجد العديد من الخدمات الأولية التي يجب أن تقدمها أي شبكة محلية (مخدّم الملفات File Server، البريد الإلكتروني E-mail، النفاذ إلى شبكة الوب العالمية WWW Access)، مما يؤدي إلى تشابه بنيوي بين مختلف أنظمة التشغيل الشبكية.

وتقع نظم التشغيل الشبكية في مجموعتين أساسيتين تختلفان في طريقة تخديم المستخدمين، حيث تتّبع المجموعة الأولى نظام تخديم مبني على أساس نموذج زبون/مخدّم (Client/Server)، ويتميز هذا النموذج بوجود حاسوب وحيد يزوّد مستخدمي الشبكة المحلية بكل خدمة مطلوبة، ويسمى هذا الحاسوب بالمخدّم، يكون هذا الحاسوب، من أجل خدمة معينة، مزوّداً ببرمجيات خاصة بهذه الخدمة تضمن تقديمها للمستخدمين، ومن ناحية أخرى، يجب أن يُزود كل حاسوب عبر الشبكة المحلية ببرمجيات تمكنه من النفاذ إلى تطبيقات هذا المخدّم والحصول على الخدمة المطلوبة، وفي هذه الحالة يدعى الحاسوب الذي يطلب الخدمة بالزبون. في حين تتّبع المجموعة الثانية نظاماً آخر

يدعى نظام الندّ للندّ (Peer-to-Peer)، حيث يمكن لأي حاسوب مربوط إلى الشبكة أن يلعب دور المخدّم ويزود الشبكة بمختلف التطبيقات الخدمية.

يجري اختيار نظام تشغيل الشبكة المحلية عند بنائها من إحدى المجموعتين السابقتين، وذلك بحسب نوعية الخدمات التي سوف تقدمها هذه الشبكة من جهة، ووفقاً لحجم الشبكة وعدد محطاتها من جهة أخرى، فإذا كانت هذه الشبكة تضم عدداً قليلاً من المستخدمين المشتركين في موردٍ ما والراغبين بالتشارك في الملفات فقط، فإن نظام التشغيل المعتمد على نظام الندّ للندّ قادر على تلبية هذه الخدمات. أما في حالة شبكة محلية تضم عدداً كبيراً من المستخدمين وتقدم خدمات تجارية أو مصرفية أو غيرها من الخدمات عالية المستوى، فإن نظام التشغيل زبون/مخدّم يكون هو الحل.

وهناك خمسة نظم تعتبر من أهم نظم التشغيل المعتمدة في الشبكات المحلية حالياً، وسنستعرضها فيما يلي:

2-4-1 نظام NETWare

قامت شركة Novell بتصميم نظام تشغيل الشبكات NETWare في الثمانينيات، ويتميّز هذا النظام بالتعامل الأساسي مع سطح المكتب في الحواسيب الشخصية (PCs) التي كانت قد بدأت تنتشر انتشاراً كبيراً في تلك الفترة وأصبحت تستخدم بكثرة في بناء الشبكات المحلية التي كانت صغيرة الحجم نسبياً وتضم عدداً قليلاً من الحواسيب، كما كانت ذات متطلبات قليلة.

وبدأ النظام NETWare منذ ذلك الحين بالتطور على نحوٍ هائل ليوافق الاتساع المطّرد في حجوم الشبكات المحلية وتطور خدماتها، وبدأ بدعم نظم النفاذ من الحواسيب الشخصية إلى حواسيب Macintosh وحواسيب Unix، حتى أصبح يعتبر نظام التشغيل المسيطر في الشبكات المحلية، حيث أنه كان في إحدى الفترات نظام التشغيل المعتمد في 70٪ من الشبكات المحلية.

يمتاز النظام NETWare بإمكانية تخديم عدد هائل من المستخدمين باعتماد نموذج زبون/مخدّم، وبإمكانية دعم مختلف الشبكات المحلية التي تستخدم حواسيبَ شخصية أو حواسيب Macintosh

أو Unix، كما أنه يمتاز بإمكانية النفاذ إلى شبكة الإنترنت بواسطة البروتوكول TCP/IP، وهو ملائم لمختلف البنى الفيزيائية للشبكات المحلية (شبكة إثرنت، الشبكة الحلقية، الشبكة الخطية، وشبكة FDDI).

2-4-2 نظام Windows NT

يُعتبر هذا النظام المصمم من قبل شركة مايكروسوفت (Microsoft) المنافسَ الأقوى للنظام NETWare، فهو مشابه جداً له من حيث استخدام نموذج زبون/مخدّم، ومن حيث ملاءمته لمختلف أنواع الشبكات المحلية، وهو ذو أداء جيد، ويعتبر أقل كلفة وأسهل استخداماً.

2-4-3 نظام Windows لمجموعات العمل

يعتمد نظام التشغيل (Windows for Workgroups) على محيط شبكة الندّ للندّ ويعتبر نظامَ تشغيل جيد للشبكات المحلية الصغيرة نسبياً، حيث أنه يقدم الخدمات الأساسية البسيطة فقط كالتشارك في الملفات والطابعات والتطبيقات. ويعتبر رخيصاً جداً بالمقارنة مع نظم زبون/مخدّم المستخدمة في الشبكات المحلية الكبيرة، إلا أنه لا يستطيع أن يقدم الخدمات الهائلة التي تقدمها من حيث أمن الشبكة والخدمات عالية الطبقة.

2-4-4 نظام LANtastic

يعتمد نظام التشغيل LANtastic أيضاً على محيط شبكة الندّ للندّ ويعتبر نظاماً ملائماً للشبكات المحلية الصغيرة ومشابهاً جداً للنظام Windows for Workgroups، إلا أنه أقل انتشاراً منه بالرغم من استخدامه لبعض بروتوكولات النظام NETWare.

2-4-5 نظام Appletalk

وهو نظام تشغيل يعتمد على محيط شبكة الندّ للندّ ويدعم الشبكات المحلية الصغيرة التي تستخدم حواسيب Macintosh، ولا يعتبر نظام Appletalk مكلفاً لأنه أصبح جزءاً من نظام التشغيل الأساسي لحواسيب Macintosh، مما يسهل عملية إعداده في الشبكة.

2-5 النفاذ عن بعد في الشبكات المحلية

يُعتبر النفاذ عن بعد (Remote Access) إلى موارد الشبكات المحلية من أهم الخدمات التي تقدمها الشبكة المحلية للمستخدمين ؛ ولم تظهر هذه الخدمة مع بداية ظهور الشبكات المحلية حيث كانت هذه الشبكات في بادئ الأمر محصورة في عدة حواسيب متجاورة تتخاطب فيما بينها عن طريق نقل المعطيات الحاسوبية الرقمية مباشرة عبر الأسلاك. وعندما اتسعت الشبكات المحلية لتغطي مساحات أكبر أصبح من الضروري إيجاد وسيلة تضمن انتقال المعطيات بين الشبكة والحواسيب البعيدة مما يسمح للمستخدم البعيد بالنفاذ إلى الشبكة، وقد حُلّت هذه المشكلة باستخدام جهاز الوديم Modem الذي استطاع تأمين عملية النفاذ عن بعد للمستخدمين الذين أصبحوا قادرين على التخاطب مع مخدّمات الشبكة المحلية من أماكن بعيدة.

وقد تطورت خدمة النفاذ عن بعد في الشبكات المحلية تطوّراً هائلاً بسبب انتشار أجهزة الوديم السريعة وتطور هذه الأجهزة وانتشار بروتوكولات جديدة تدعم هذه الخدمة مثل بروتوكول PPP (Point-to-Point Protocol)، إضافةً إلى التطور الهائل في مجال الشبكات الهاتفية التي تعمل كوسط نقل للمعطيات في عملية النفاذ عن بعد وفي ربط الشبكات المحلية، ولعل أهم هذه التطورات في الشبكات الهاتفية ظهور شبكة الخدمات المتكاملة الرقمية ISDN (Integrated Services Digital Networks).

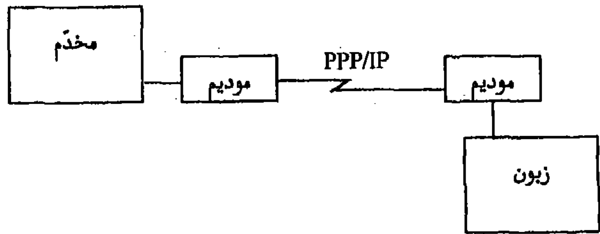
منذ عدة سنوات كان المستخدم البعيد قادراً على الوصول إلى مخدّم الملفات في الشبكة المحلية بسرعة 2400Bps فقط، ولم يكن بالإمكان سوى استعراض النصوص فقط إضافةً إلى القيام ببعض العمليات المحدودة، أما الآن فقد أصبح بالإمكان تبادل الملفات والصور بسبب التطور الكبير في مجال تخديم المستخدم البعيد المنسوب إلى أجهزة الموديم وشبكات النقل الرقمية ISDN.

2-5-1 أجهزة الموديم

جهاز الموديم هو جهاز تعديل/ فك تعديل، وكلمة MODEM مشتقة من تجميع الحروف الأولى من عبارة (MOdulation/DEModulation) في اللغة الإنكليزية.

تجري عملية وصل المستخدم البعيد إلى مخدّمات الشبكة المحلية عن طريق خطوط الهاتف، وذلك باستخدام أجهزة الموديم التي تعتبر بمنزلة أجهزة الهاتف لحواسيب الشبكة. فلتحقيق عملية النفاذ عن بعد من قبل أحد الحواسيب البعيدة إلى أحد مخدّمات الشبكة المحلية لا بد من وجود جهاز موديم في كل طرف من طرفي الاتصال بحيث يعمل الجهازان ثنائياً على الموافقة بين الحاسوب في كل طرف وخط الهاتف المستخدم كما يُظهر ذلك الشكل (2-14).

يقوم جهاز الموديم في طرف الإرسال بتحويل الإشارة الرقمية المستخدمة في الحاسوب (سلسلة من الأصفار والوحدان) إلى إشارة تمثيلية (Analog) كهربائية مستمرة زمنياً وتأخذ عدداً لا منتهياً من القيم، وذلك للتلاؤم مع النقل عبر الخطوط الهاتفية التي تُعرّض الإشارات الرقمية إلى التشويه والضياع إذا جرى نقلها مباشرة دون عملية التحويل، أما في طرف الاستقبال فيقوم الجهاز بعملية التحويل العكسية.



الشكل (2-14): آلية استخدام المودم في الاتصال

يوصل جهاز الموديم إلى الحاسوب عن طريق بوابة خاصة تدعى البوابة التسلسلية (Com Port)، ويوصل من الجهة الأخرى إلى مخرج الهاتف بالطريقة نفسها التي يوصل بها أي جهاز هاتف. ويقوم جهاز الموديم بنقل المعطيات عبر الشبكة الهاتفية بسرعة تعد بطيئة جداً إذا ما قورنت بسرعة النقل للمسافات القريبة التي لا تستدعي عمليات التعديل وفك التعديل، مما يحدّ من الخدمات التي يمكن تقديمها للمستخدم البعيد. ولا يمكن الهروب من هذا البطء في سرعة جهاز الموديم (التي لا تتجاوز 28.8 KBps، في حين تبلغ سرعة بطاقة إثرنت عادية مثلاً 10 MBps)، وهذه المحدودية في السرعة ناجمة عن الوقت اللازم لإجراء عمليات التعديل وفك التعديل.

للتحكم في عملية النفاذ عن بعد إلى مخدّمات الشبكة تستخدم الشبكة المحلية مخدّماً خاصاً يدعى بمخدّم الاتصال (Comm Server) أو بالعبر (Gateway)، وتجري جميع عمليات النفاذ عن بعد عبر هذا المخدّم المجهّز بجهاز موديم وبرمجيات خاصة. فعندما يطلب أحد الحواسيب البعيدة أحد مخدّمات الشبكة المحلية عبر جهاز الموديم الخاص به تجري عملية الاتصال المطلوبة من قبل المستخدم مع مخدّم الاتصال أولاً (المجهز بجهاز الموديم)، حيث يلعب دور المخدّم المطلوب من جهة الحاسوب البعيد، ودور الزبون بالنسبة للمخدّم المطلوب، وتجري عملية تمرير الخدمة المطلوبة من المخدّم المطلوب إلى مخدّم الاتصال ومن ثم من مخدّم الاتصال إلى الحاسوب البعيد.

يمكن إعداد العديد من المخدّمات في الشبكة المحلية (مخدّم الملفات مثلاً) لتكون مخدّمات اتصال، وهذا يوفر في الوقت طبعاً ولكنه يسبب بالتأكيد مخاطر أمنية لا يستهان بها على الشبكة المحلية، التي سيكون من الأفضل لها أن تحافظ على استقلالية مخدّم الاتصال في هذه الحالة.

تستخدم تقنية مخدّم الاتصال في الشبكات المحلية الصغيرة، فهو غير قادر بالطبع على تخديم عدد كبير من المستخدمين عن بعد بواسطة جهاز موديم وحيد، حيث نستخدم في الشبكات المحلية الكبيرة تقنيةً مختلفة في التخديم باستخدام مخدّم اتصال أفضل يُسمى المخدّم الطرفي، وعدة أجهزة موديم (Modem Bank and Terminal Server). يمتاز هذا المخدّم بقدرته على الاتصال بواسطة عدة أجهزة موديم كل منها موصول إلى خط هاتفي، فعندما تزداد طلبات التخديم البعيدة عبر الشبكة يقوم هذا المخدّم باستخدام أجهزة موديم جديدة.

تُقدم الشبكات المحلية حالياً خدمة النفاذ عن بعد للحواسيب البعيدة بإعطائها عنواناً يخص الشبكة المحلية نفسها خلال عملية الاتصال، مما يسمح لهذه الحواسيب بالاتصال مباشرة مع مخدّمات الشبكة وذلك باستخدام البروتوكول PPP الذي يمكّن الحاسوب المتصل عن بعد من لعب دور الزبون في الشبكة المحلية والاستفادة من خدماتها كما لو أنه إحدى المحطات المباشرة، وتدعى هذه الطريقة بنفاذ الزبون عن بعد (Remote Client Access).

2-5-2 شبكات الخدمات المتكاملة الرقمية ISDN

تقدم شبكات النقل الرقمية ISDN خدمات النقل الرقمية إلى الشبكات المحلية التي تغدو غير مضطرة لاستخدام أجهزة الموديم لتحويل الإشارات الرقمية إلى تمثيلية، إذ أصبح من الممكن إرسال المعطيات الرقمية مباشرة عبر خطوط الهاتف باستخدام شبكات ISDN، وبسرعات نقل تفوق سرعة نقل جهاز الموديم، إذ تبلغ أدنى سرعة نقل في شبكات ISDN 64 KBps وتزيد سرعتها القصوى عن 1 MBps.

يعتمد نمط التجهيزات الخاص بوصل الشبكة المحلية إلى شبكات ISDN على نمط واجهة شبكة ISDN الذي قد يكون من أحد النمطين التاليين:

- *واجهة معدّل النقل الأساسية (Basic Rate Interface <BRI>)*: تتكون هذه الواجهة من قناتي نقل تُسمى كلٌ منهما قناة B (Bearer)، وتستطيع قناة B نقل المعطيات الرقمية بسرعة 64 KBps، وعند استخدام القناتين معاً يمكن الوصول إلى معدّل نقل 128 KBps. وتحتاج هذه الواجهة إلى محول طرفي (Terminal Adapter) لوصلها إلى جهاز الحاسوب بدلاً من جهاز الموديم.

- واجهة معدل النقل الأولية (Primary Rate Interface <PRI>): تتكون هذه الواجهة من 24 قناة من النوع B لتشكل خط نقل رقمي بسرعة 1.5 MBps. وتحتاج عملية ربط هذا الخط بالحاسوب إلى تجهيزات أكثر تعقيداً من تلك التي نحتاجها في حالة الواجهة الأولى BRI، ليتمكن الخط من فرز وتركيب معطيات القنوات المكونة له.

يُجهّز مخدّم الملفات في الشبكة المحلية ببطاقة ISDN وعندها تستطيع الحواسيب البعيدة الاستفادة من خدمات الشبكة باقتناء بطاقة ISDN وطلب الخدمة من الشبكة بطريقة مشابهة لحالة وجود جهاز الوديم. وكما هي الحال في المخدّم المجهّز بجهاز الوديم يمكن تجهيز المخدّم الطرفي بعدة بطاقات ISDN، كما يمكن استخدام البروتوكول PPP للمخدّم الطرفي الخاص بـ ISDN لتأمين طبقة الخدمات نفسها المقدّمة في حالة الوصل عن طريق جهاز الوديم ولكن بسرعة أكبر بكثير، مما يحسّن من زمن استجابة النفاذ عن بعد لموارد الشبكة المحلية.

الفصل الثالث

بناء الإنترانت

في الفصل الأول قمنا بعرض مفاهيم الإنترانت وفوائدها وكيفية تقدير الفائدة منها، وسنقوم في هذا الفصل بعرض المكونات الأساسية في بناء شبكات الإنترانت بعد أن بينّا في الفصل الثاني مكونات الشبكات المحلية التي تمثّل البنية التحتية لأي شبكة إنترانت. نبدأ بالمكونات الفيزيائية الإضافية لتحقيق شبكة إنترانت ومن ثم نستعرض الأدوات البرمجية المطلوب توفرها، وبعد ذلك نشرح طرق وصل الإنترانت مع شبكة الإنترنت العالية، وبذلك نكون قد بينّا الصورة الكاملة لبناء شبكة إنترانت.

3-1 بناء الإنترانت الفيزيائي

يمكن أن تكون الإنترانت (خصوصاً في مؤسسة كبيرة) ذات بنية معقدة تحتوي على العديد من الشبكات الفرعية التي تضم الشبكات المحلية في كل قسم من أقسام المؤسسة وكذلك شبكات فرعية أكبر حجماً وتتكون أساساً من مجموعة من الشبكات ؛ ومن ثم فإن وصل الشبكات المتباعدة يعتبر من المتطلبات الأساسية في بناء أي شبكة إنترانت.

نستخدم لتحقيق الوصل الفيزيائي تجهيزات خاصة تُسمى الجسور (Bridges) والموجهات (Routers)، وسنقوم فيما يلي بشرح هذه المكونات الفيزيائية، وأماكن استخدامها.

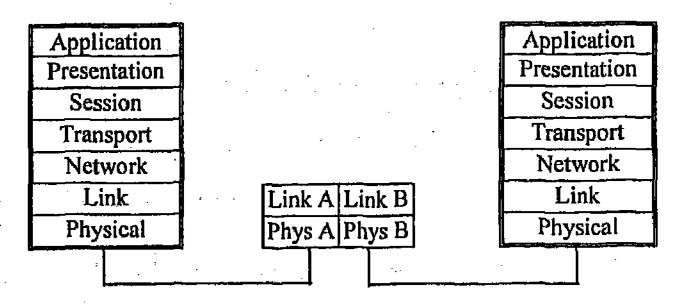
3-1-1 الجسور

الوظيفة والبنية

الجسور هي مجموعة من البنى المادية (العتاد) والبرمجيات تقوم بوظيفة وصل الشبكات المحلية المختلفة لتكوين شبكة واحدة هي شبكة الإنترانت. ولكنها لا تستخدم للوصل بين شبكات كاملة، حيث نحتاج في هذه الحالة إلى الموجهات وليس إلى الجسور، كما هو الحال عند وصل شبكة إنترانت مع شبكة الإنترنت، أو وصل شبكة إنترانت مع شبكة إنترانت أخرى.

تعمل الجسور ضمن طبقة الوصل في نموذج OSI/OSI حيث تقوم عموماً بتخزين الإطارات المستقبلة في جهةٍ ومن ثم تنسخها على الجهة الأخرى. وقد كانت الجسور في مراحل تطويرها الأولى غير قادرة على وصل الشبكات غير المتوافقة طبولوجياً، إذ كانت تعمل على جزء التحكم بالنفاذ إلى الوسائط (MAC) في طبقة وصل المعطيات (مثلاً تختلف بنية شبكة إثرنت عن بنية الشبكة الحلقية في هذا الجزء نظراً لعدم توافقهما)، ولذلك تعمل الجسور الحديثة على جزء التحكم بالوصلة المنطقية LLC (Logical Link Control) في طبقة وصل المعطيات، فإذا كانت الشبكتان تستخدمان بروتوكول الاتصال نفسه (مثلاً IPX في كلتا الشبكتين) فإنه يصبح بالإمكان وصل الشبكتين بواسطة الجسور.

كما يمكن استخدام الجسور أيضاً للوصل بين الشبكات وصلاً غير مباشر بخطوط بعيدة المدى (تكون مؤجرة عادةً (Leased Lines)).



الشكل (3-1): بنية الجسور

مبدأ العمل

- *الجسور في شبكة إثرنت:* تستخدم الجسور في شبكات إثرنت تقنية توجيه شفافة لمعالجة النقل عبر الشبكة. فمن خلال عنوان الهدف في طرد المعطيات يتم اتخاذ الفعل المناسب ؛ فإذا كان هذا العنوان ينتمي إلى الشبكة نفسها فإن الجسر يتجاهل هذا الطرد، أي أن الجسور لا تمرر إلا الطرود الذاهبة إلى شبكات أخرى.
- *الجسور في الشبكة الحلقية:* تعمل الجسور في الشبكة الحلقية (Token Ring) بطريقة مختلفة فهي تستخدم طريقة التوجيه بالمصدر (Source Routing) ؛ في هذه الحالة تستخدم الجسور رسالة اختبار لحساب أفضل المسارات بين المصدر والهدف.

وعموماً، لتمرير أو عدم تمرير طرد ما من خلال جسر ما، يستخدم هذا الجسر جدولاً يتألف أساساً من قائمة عناوين، تبنى في البداية يدوياً، الأمر الذي يقود إلى ضرورة مراجعة هذه القوائم في كل مرة يجري فيها إضافة أو تبديل عنوان NIC في الشبكة، مما يؤدي إلى تطوير جسور قادرة على التعلم، وهي جسور مزودة ببرمجيات خاصة لتنفيذ عدد من الخوارزميات (مثل خوارزمية Spanning Tree أو خوارزمية Source Routing المُشار إليها سابقاً) التي يمكنها تحديد التغيرات في الشبكة، ومن ثم تبني الجداول آلياً. تبني الجسور الحالية قوائمها الخاصة وتعدلها آلياً من خلال مراقبة حركة النقل في الشبكة وفحص عنوان المصدر في الطرود. بقي أن نذكر أن الجسور ليست بحاجة لعنوان على الشبكة.

عمل الجسور في الإنترانت

عندما تكون حركة نقل المعطيات كبيرة في شبكة إثرنت محلية (Ethernet LAN) فإن الطرود قد تتصادم بعضها مع بعض، مما يؤدي إلى إبطاء حركة النقل في الشبكة، ويعود السبب في هذه التصادمات إلى أن جميع المعطيات تنتقل إلى جميع المحطات على الشبكة. وللتخفيض من شدة التصادمات، يمكن أن نقسّم الشبكة المحلية الواحدة إلى العديد من الشبكات الفرعية، بحيث نحصر

جُلّ حركة النقل في إحدى الشبكات الفرعية، ولا داعي للمرور كل مرة في جميع المحطات على الشبكة، وبهذه الطريقة سيقل عدد التصادمات. نستخدم الجسور أيضاً للوصل بين الشبكات الفرعية، فهي لا تسمح بانتقال المعطيات ما لم تكن متجهةً نحو شبكة أخرى، وتبقي جميع المعطيات المنقولة في الشبكة الفرعية الواحدة ضمن حدود هذه الشبكة.

إن كل إطار ينتقل عبر شبكة الإنترانت يحتوي إضافةً إلى طرد IP على معلومات تخص الطبقة الفيزيائية المبنية عليها الشبكة، تفحص الجسور هذا الجزء من المعلومات وترسل الطرد إلى العنوان المطلوب في الشبكة المحلية.

يمكن أن تربط الجسور بين شبكات الاتصال المحلية بعدة طرق، يمكن مثلاً ربط هذه الشبكات باستخدام وصلات تسلسلية عبر خطوط الهاتف العادية وأجهزة المودم، أو عبر خطوط ISDN، أو عبر خط وصل مباشر ؛ وتستخدم وحدات CSU/DSU لوصل الجسور إلى خطوط الهاتف من أجل الاتصالات البعيدة.

من السهل إعداد الجسور وصيانتها، وهي تعمل بسرعة نوعاً ما باعتبار أنها لا تقوم إلا بعملية تمرير الطرد أو إيقافه، في الفقرة التالية سوف نقوم بعرض لنوع آخر من التجهيزات المشابهة للجسور ولكنها أكثر تعقيداً، وهي الموجهات، ففي حين تستخدم الجسور للتخفيف من شدة حركة النقل في الشبكة، فإن الموجهات تستخدم عادة لوصل الشبكات أو أجزاء الشبكات فيما بينها.

3-1-2 الموجهات

الغاية من الموجهات

تضمن الموجهات إيصال المعلومات إلى وجهتها عبر أفضل طريق ممكن، كما أنها تستطيع أن تنظم حركة نقل المعطيات عبر الشبكة وتستخدم العديد من الخوارزميات في التوجيه من خلال مجموعة من البروتوكولات تدعى بروتوكولات التوجيه، كما تضمن عملية نقل المعطيات بين الشبكات غير المتوافقة

في الطبولوجيا وكذلك بين الشبكات غير المتوافقة في البرتوكولات العاملة في كل منـها، كما تستخدم الموجهات للوصل مع شبكة الإنترنت وهو ما سنقوم بعرضه في الجزء الأخير من هذا الفصل.

تختلف الموجهات الممكن استخدامها في درجة تعقيدها، والعوامـل الـتي تحـدد الموجّـه الـذي يجـب استخدامه تتعلق بالأمور التالية:

- حجم الإنترانت.
- نمط ونوعية أجزاء الشبكة.
- درجة الأمن المطلوبة.

ويمكن القول عموماً إنه كلما ازداد تعقيد شبكة الإنترانت، وازداد عدد الأماكن المختلفة التي يمكن أن ترسل إليها المعطيات، كلما ازدادت الحاجة إلى موجهات أكثر تعقيداً مـن ناحيـة التكويـن في البنيـة المادية أو البرمجية.

مبدأ العمل

عند بدء تشغيل الموجه، يجري تشغيل إجراء برمجي يُسمى إجراء التوجيه، يقوم هذا الإجراء بالأمور التالية من أجل كل طرد IP يتم استقباله:

1- يفحص الطرد ويستخلص عنوان الهدف من ترويسة الطرد IP.

2- يقوم بتحديد أفضل طريق لإرسال هذا الطرد إلى العنوان الهدف.

3- يرسل الطرد إلى الهدف عبر الطريق المحدد.

ولتحديد طريق الطرد يستخدم الإجراء قاعدة معطيات (DataBase) تُسـمى جـدول التوجيـه (سيأتي تفصيلها لاحقاً)، وتمكن من خلالها معرفة الطريق الأفضل بحسب عنوان الهدف.

إذا كان الهدف موجوداً على جزء الشبكة الذي ينتمي إليه الموجه، فإن الموجه يقوم بإرسال الطرد إلى الحاسوب المقصود، أما إذا كانت وجهة الطرد إلى شبكة جزئية أخرى أو إلى شبكة إنترانت أخرى فإن الموجه يأخذ بعين الاعتبار العديد من العوامل في تحديد الطريق الأفضل، مثل: ضغط النقل على الطرق ؛ عدد نقاط الوصل بين المصدر والهدف (ونقصد بها عدد الموجهات أو البوابات التي يمر بها الطرد في طريقه من المصدر نحو الهدف)، وبما أن الطرد IP يحتوي في أحد أجزائه على عدد نقاط الوصل، فبالتالي يجب على الموجه ألا يستخدم طريقاً يزيد فيه عدد نقاط الوصل عن العدد الموجود في الطرد IP. كما أن وجود أكثر من طريق يحقق هذا الشرط هو أمر مرغوب فيه في شبكات الإنترانت، وذلك لضمان التعدد في الطرق وبالتالي تستطيع المعطيات النفاذ في حالة انشغال بعض الطرق.

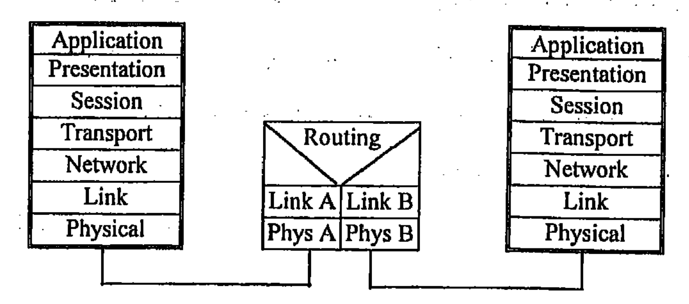
قد يجري في بعض الأحيان إرسال الطرود إلى بوابة دخل ما في موجه بسرعة تتجاوز قدرتها على معالجة هذه الطرود، في هذه الحالة تُخزن الطرود في منطقة معينة من ذاكرة الموجه RAM تُسمى خط انتظار (Queue) الدخل، ولكل بوابة دخل خط الانتظار الخاص بها، أي يمكن أن يملك الموجه أكثر من خط انتظار دخل ؛ في هذه الحالة يقوم الموجه بمعالجة الطرود في خط انتظار الدخل حسب ترتيب ورودها.

إذا كان ضغط النقل على الموجه كبيراً بحيث يتجاوز حجم الطرود التي يجب تخزينها الحجم المخصص لخط الانتظار (نسمي حجم خط الانتظار التخزيني طولَ الخط)، في مثل هذه الحالة يجري إهمال بعض الطرود التي لا يستطيع الموجه معالجتها وبالتالي فإن هذه الطرود لن ترسل إلى هدفها، لكن هذا لا يعني ضياعاً في المعلومات، لأن بروتوكول النقل TCP يأخذ بعين الاعتبار الضياع في الطرود على الطريق فإذا لم تصل جميع الطرود إلى الهدف فإنه يطلب إعادة إرسالها حتى تصل جميعها.

البنية

يملك كل موجه أكثر من بوابة فيزيائية: بوابات دخل لاستقبال المعطيات وبوابات خرج لإرسال المعطيات، وتكون هذه البوابات ثنائية الاتجاه، أي أنها يمكن أن ترسل وتستقبل، وتعمل الموجهات

على مستوى طبقة الشبكة في نموذج ISO/OSI وهذا ما يميّزها عن الجسور، ويجعلها قادرة على التحكم بعناوين IP للطرود.



الشكل (3-2): بنية الموجه

هناك العديد من الموجهات المبنية على أساس مادي أو برمجي، وفي بعض الحالات يمكن تشغيل العديد من البرمجيات التي تعمل كموجهات على نفس البنية المادية مثل الموجه Multi Protocol Router من شركة Novell، وهو برنامج موجّه يعمل على البنية المادية لأي موجه. في بعض الموجهات، وخاصة الموجهات عالية الأداء، يجري زرع برمجيات التوجيه مباشرة على البنية المادية.

يمكن إدارة الموجهات وتشخيص المشاكل فيها وحلها باستخدام برمجيات معينة مثل بروتوكول SNMP (Simple Network Management Protocol). نشأ هذا البروتوكول من حاجة مديري الشبكات لتشخيص ومعالجة مشاكل الشبكة عن بعد، حيث يقدم هذا البروتوكول العديد من الأدوات لمراقبة وتعديل تشكيل الشبكة عن بعد. لكن النسخة الأولى من هذا البروتوكول لم تأخذ بعين الاعتبار مسألة التحقق من الهوية، ولذلك يصبح نظرياً بإمكان أي شخص تعديل تشكيل الشبكة، ومن ثم فإن العديد من بائعي البرمجيات يعطّلون قدرات البروتوكول على التعديل. لكن البرتوكول SNMPv2 يأخذ بعين الاعتبار مسألة التحقق من الهوية (انظر RFC 1157 لمزيد من التفاصيل).

جداول التوجيه

لا تختلف هذه الجداول بالمضمون وإنما بطريقة البناء:

1- جدول التوجيه الأصغري

يستخدم في أبسط أنواع شبكات الإنترانت، وكذلك في شبكات الإنترانت المؤلفة من شبكة TCP/IP واحدة، أو عندما تكون هذه الشبكة موصولة بشبكة TCP/IP أخرى أو بالإنترنت. في التوجيه الأصغري يقوم برنامج يدعى بـ ifconfig بخلق جدول التوجيه آلياً، ويتألف الجدول في هذه الحالة من عدد قليل من المداخل الأساسية. وبما أن عدد الأماكن التي يمكن أن ترسل إليها المعطيات محدود فإننا بحاجة لتهيئة عدد أصغري من الطرق فقط.

2- جدول التوجيه الثابت

يستخدم إذا كانت الشبكة تتألف من عدد محدد من شبكات TCP/IP الجزئية. يجري في هذه الحالة إرسال الطرود ذات العناوين المحددة إلى موجهات محددة، ولا تغير الموجهات من وجهة الطرود المحددة في الجداول عند تغير حركة النقل على الشبكة، أي أن الجداول الثابتة يجب ألاّ تُستخدم إلاّ في حالة وجود طريق واحد لكل هدف معطى. يسمح جدول التوجيه الثابت لمدير الشبكة بإضافة المداخل إلى الجدول وحذفها.

3- جدول التوجيه الديناميكي

تعتبر هذه الجداول من أكثر جداول التوجيه تعقيداً، ومن الضروري استخدامها عندما يكون هناك أكثر من طريق يمكن أن تُرسل عليه المعطيات نحو الهدف. وفي شبكات الإنترانت الأكثر تعقيداً تتغير هذه الجداول باستمرار مع تغير حركة النقل على الشبكة، وتتغير أيضاً مع تغير شروط هذه الشبكة، ومن ثم فإنها توجه المعطيات أفضلَ توجيهٍ ممكن آخذة بعين الاعتبار الحالة الحالية لحركة النقل على شبكة الإنترانت.

يجري بناء جداول التوجيه الديناميكية بواسطة بروتوكولات التوجيه، حيث تتبادل الموجهات المعلومات عن أفضل الطرق في توجيه المعطيات ضمن الحالة الفعلية للإنترانت، وبإمكان الموجه ذي جدول التوجيه الديناميكي أن يغير طريق المعطيات إلى طريق احتياطي عندما يكون الطريق الرئيسي

معطلاً لسبب ما. كما بإمكانه تحديد أفضل طريق يمكن أن تسلكه المعطيات نحو هدفها. توزع الموجهات عناوين IP التي تخصها وتتعرف على عناوين الموجهات المجاورة، ويجري استخدام هذه المعلومات في خوارزميات معروفة تستطيع الموجهات من خلالها حساب أفضل طريق لإرسال الطرود.

بروتوكولات التوجيه

تستخدم هذه البروتوكولات الموجهات في التخاطب فيما بينها، وتقسم إلى نوعين: بروتوكولات التوجيه الداخلية، وبروتوكولات التوجيه الخارجية.

يوجد بالنسبة للنوع الأول ثلاثة بروتوكولات رئيسية كثيرة الاستخدام هي:

- RIP (Routing Information Protocol) يعتمد على خوارزمية Distance Vector.
- OSPF (Open Shortest Path First) يعتمد على خوارزمية Link State.
- IGRP (Cisco's Propriety Interior Gateway Routing Protocol) يعتمد على خوارزمية Distance Vector.

أمّا بالنسبة لبروتوكولات التوجيه الخارجي فيوجد البروتوكلان التاليان:

- EGP (Exterior Gateway Protocol).
- BGP.

ولشرح هذين النوعين سنكتفي بعرض البروتوكولات التالية:

- بروتوكول RIP: أكثر البروتوكولات استخداماً، يقوم هذا البروتوكول بتحديد أفضل طريق لتوجيه المعطيات عن طريق حساب عدد نقاط الوصل على الطرق المكنة، ويختار دائماً الطريق الذي يحتوي على أقل عدد من نقاط الوصل، ويستبعد هذا البروتوكول الطرق التي تحتوي على نقاط وصل تتجاوز 16 نقطة، وفي أغلب شبكات الإنترانت فإن هذه الافتراضات لا تسبب أية مشكلة. إن هذا البروتوكول يعتمد على تحقيق خوارزمية مشهورة في التوجيه

هي خوارزمية Distance Vector، وتحوي العديد من أنظمة التشغيل على البرمجيات التي تحقق هذا البروتوكول، فمثلاً في نظام التشغيل BSD UNIX هذا البروتوكول محقق من خلال برنامج "routd".

- بروتوكول EGP: يستخدم هذا البروتوكول في شبكة الإنترنت، حيث يكون هناك العديد من الموجهات التي يجب على المعطيات أن تتجاوزها لتصل إلى الهدف، وقد لا نحتاجه على شبكة الإنترانت لأنه من النادر أن تكون هذه الشبكة واسعة بحيث يكون هناك 16 نقطة وصل قد تجتازها المعطيات للوصول إلى الهدف.

يمكن أن تستخدم شبكة الإنترانت الواحدة أكثر من تقنية في التوجيه، وذلك بحسب حاجات الشبكات الجزئية، فقد تستخدم بعض الأجزاء موجهات بجداول ثابتة، في حين تحتاج أجزاء أخرى إلى موجهات بجداول ديناميكية، ودائماً يكون الخيار لصالح جعل الإنترانت أكثر مرونة.

ملاحظة

يجري أحياناً وضع الجسور والموجهات في نفس العتاد ويُسمى Brouter، حيث يجمع هذا العتاد بين وظائف الجسور والموجهات في المنتج نفسه. إذا كانت المعطيات تتجه إلى شبكة LAN أخرى ضمن الشبكة نفسها أو إلى شبكة جزئية فإن Brouter سيتصرف كجسر وتُرسل المعطيات حسب عنوان الإثرنت، أما إذا لزم إرسال المعطيات إلى شبكة أخرى تماماً فإن Brouter سيتصرف كموجه ويقوم بتوجيه المعطيات حسب عنوان IP.

3-2 بناء الإنترانت البرمجي

بعد أن ناقشنا كيفية تجهيز شبكة فيزيائية للإنترانت من خلال ربط عدة شبكات محلية، سنقوم فيما يأتي بعرض البنية البرمجية لهذه الشبكة، أي كيفية إجراء الاتصالات بين الحواسيب في الإنترانت

من وجهة نظر برمجية. كما سنتعرض لمفهوم أساسي تعتمد عليه معظم التطبيقات في الإنترنت والإنترانت، ثم نعرض متطلبات تحقيق هذا المفهوم

3-2-1 مفهوم زبون/مخدّم

إن معظم تقنيات الإنترنت مبنية على أساس الاتصال وفق مفهوم زبون/مخدّم، وبما أن الإنترانت هي تطبيق لتقنيات الإنترنت على الشبكات المحلية، فإننا سنقوم فيما يلي بتوضيح هذا المفهوم وكيفية نشوئه.

لمحة تاريخية

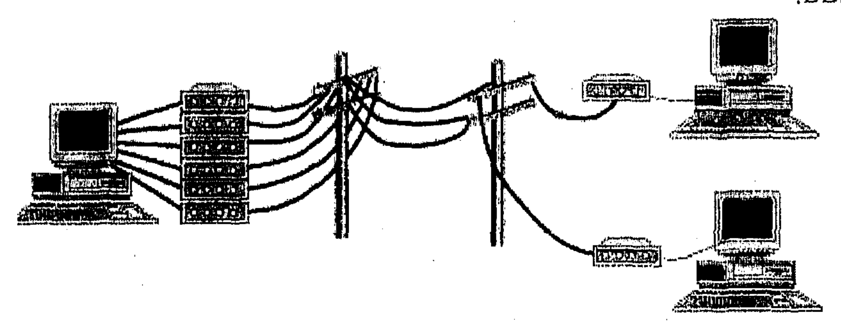
قبل انتشار الحواسيب الشخصية في بداية الثمانينيات كانت الحكومات والمؤسسات تقوم بالمهام المعلوماتية على حواسيب كبيرة (Mainframes). امتلكت هذه الحواسيب القدرة على الحساب ولكنها كانت بطيئة، ولا تستطيع التعامل إلا مع عدد محدود من المستخدمين عن طريق الطرفيات التي تتألف أساساً من لوحة مفاتيح وشاشة عرض. ومع ظهور الحواسيب الشخصية منذ العام 1985 في عالم الأعمال حلت هذه الحواسيب مكان Mainframes على الرغم من أن إمكاناتها كانت مسخرةً لمستخدم وحيد، ولكن تبادل المعطيات ظل صعباً على الرغم من الوظائف المتعددة التي استطاعت الحواسيب الشخصية القيام بها، لأن التشارك بالمعلومات كان فيزيائياً، حيث كان لا بد من نسخ الملفات على قرص مرن لنقلها إلى حاسوب آخر عبر سواقة القرص المرن. وكانت الشبكات المحلية حلاً جزئياً لمشكلة الاتصال بين الحواسيب الشخصية حيث أصبح بالإمكان وصل الحواسيب المختلفة في مبنى واحد عن طريق الأسلاك، وأصبح بإمكان المستخدمين التشارك في الملفات دون الحاجة إلى تثبيتها على حواسيبهم الشخصية، لكن في لحظة معينة لا يمكن إلا لمستخدم واحد الوصول إلى الملف.

ولكن التشارك على الملفات لم يحل مشكلة تبادل المعطيات، حيث لم يؤدِ إلى التخلص من الحاجة إلى التخزين الورقي والتكاليف المترتبة عليه. وقد سهل ظهور خدمة البريد الإلكتروني على الشبكات

المحلية في أواخر الثمانينيات الاتصالات الداخلية، ولكنه لم يحل مشكلة الاتصالات الخارجية مع شبكات أخرى.

أستخدِم الوديم في الاتصالات بين الحواسيب لأول مرة في السبعينيات، لكنه لم يكتسب سمعة حسنة إلاّ في منتصف الثمانينيات، إذ أصبح بإمكان الحواسيب في المواقع البعيدة الاتصال فيما بينها. أي أصبح بإمكان شخصين تبادل الملفات والتحدث فيما بينها آنياً عبر هذه الوصلة، لكن وصلة الموديم الأولية كانت خطية وبالتالي محدودة النطاق ولا يمكن إلا لمستخدمين اثنين فقط الاستفادة منها، مما أدى إلى ظهور أنظمة اللوحات الإعلانية BBS (Bulletin Board Systems) لتحسين قدرات الموديم، حيث مكنت أنظمة BBS المستخدم من الاتصال مع عدد كبير من المستخدمين في مواقع بعيدة وتبادل المعلومات عبر وصلة الموديم.

عبّرت برمجيات BBS عن ظهور المعالم الأولى لتطبيقات زبون/مخدّم، وقد تكوّن الشكل الأولي لهذا المفهوم من حاسوب رئيسي يستطيع الاتصال مع بضع مئات من الموديمات، وعلى الجهة الأخرى من الوصلة يوجد المستخدمون النهائيون، حيث يطلب المستخدم النهائي الحاسوب الرئيسي في BBS عن طريق الموديم الخاص به ليُصار إلى وصله إلى أحد موديمات BBS. إن نظام BBS بني على أساس فكرة بسيطة ؛ وهي أن ننشئ خزاناً للمعلومات على حاسوب واحد ونسمح للجميع بالولوج إليه ليصبح مكاناً لاجتماع وتبادل الأفكار والمعلومات، ولقد كان مفهوم المخدّم هو أساس النجاح لأنظمة BBS.



الشكل (3-3): نظام BBS

في بداية تطبيق هذا النظام كان على المستخدم كتابة العديد من الأوامر للحصول على الاتصال، ثم ظهرت بعد ذلك واجهات تخاطب بيانية تسهل عملية الاتصال، وبسبب التنوع الكبير في الحواسيب الشخصية في ذلك الوقت (مثل Amiga، Atari، Commador، Texas Instruments، إضافةً إلى IBM و Apple) والتنوع الكبير في أنظمة التشغيل الخاصة بكل منها، فإن عملية إجراء الوصل عن طريق نظام BBS واجهت بعض المشاكل، فلم يكن بمقدور هذا النظام بالطبع معرفة نوع الحاسوب الذي يقوم بالاتصال، وبالتالي كان على نظام BBS بناء واجهة مشتركة يستطيع أي حاسوب إجراء الاتصال من خلالها. وتعتبر الواجهة ANSI/VT-100 من أولى هذه الواجهات، وهي لا تزال مستعملة حتى الآن، حيث تسمح لأي حاسوب مهما كان نوعه بالاتصال من أي مكان للحصول على واجهة مشتركة.

ومع تطور البرمجيات أضيفت وظائف أخرى جديدة فأصبح بالإمكان إجراء محادثة بين المستخدمين عن طريق تبادل الرسائل، وفيما بعد أصبح بالإمكان القيام بالمحادثة الآنية، وقد سمح هذا التطور للمستخدمين بإجراء محادثة ديناميكية بدلاً من المحادثة الستاتيكية، حتى أنه أصبح بالإمكان تشغيل بعض الألعاب واللعب من خلال نظام BBS. وبدأ رجال الأعمال بالاعتماد على الحواسيب في أعمالهم مع ظهور نظام BBS، وذلك لتأمين بعض الخدمات لزبائنهم، ولتحقيق الدعم التقني للعمل.

وأصبحت أنظمة BBS الوسيلة الوحيدة للاتصال بين الحواسيب البعيدة، وبدأت هذه الأنظمة بالاتصال فيما بينها أو حتى مع الإنترنت وذلك في أواخر الثمانينيات وأوائل التسعينيات، حيث كان الاتصال مع الإنترنت يتحقق من خلال وصلة موديم عبر مزود لخدمة الإنترنت (Internet Service Provider <ISP>). وحسب مجلة Board Watch وصل عدد أنظمة BBS إلى 30,000 نظام في الولايات المتحدة الأمريكية، وفي أواخر الثمانينيات نشأت بين هذه الأنظمة العديد من الشبكات الوطنية التي أطلقت العديد من الخدمات مثل CompuServe و America On Line و Prodigy، وبدأت هذه الخدمات الخاصة باجتذاب العديد من المستخدمين.

نرى مما سبق أن /مخدّم نشأ كنتيجة طبيعية لتحقيق تبادل المعلومات بين مجموعة من المستخدمين في آن واحد ولم يظهر هذا المفهوم فجأة وإنما تطور تدريجياً عن طريق حلول مرحلية لمشكلة تبادل

المعلومات حتى أخذ شكله النهائي. وقد تبنت شبكة الإنترنت هذا المفهوم في معظم تطبيقاتها، كما ظهرت شبكات أخرى غير الإنترنت اعتمدت على هذا المفهوم مثل (UNIX User Network) <USNET> التي تعتمد البروتوكول UUCP (UNIX to UNIX Copy Protocol) وشبكة BITNET، وفي الوقت الحالي فإن هذا النموذج هو المسيطر في شبكات الإنترانت وشبكة الإنترنت.

العلاقة بين الزبون والمخدّم

المخدّم هو تطبيق برمجي مهمته استقبال استفسار ما ومعالجته ثم الإجابة عليه، ويعمل عادة على حاسوب مركزي فعّال وذي قدرة عالية على المعالجة، (يمكن حالياً استخدام الحواسيب الشخصية المتطورة كمخدّمات). يتعامل المخدّم مع عدة وصلات قادمة من عدة مصادر كل منها يمثل ما يسمى بالزبون.

تعتمد تطبيقات زبون/مخدّم على الناقلات (Transactions) البرمجية، حيث يرسل الزبون طلبه إلى المخدّم، الذي يجاوبه بناءً على المعلومات التي وصلته.

يجب أن يحتوي طلب الزبون على المعلومات التالية:

عنوان المخدم، الطلب، عنوان الزبون.

إن العلاقة بين الزبون والمخدّم غير متكافئة من حيث أن المخدّم هو الذي يقوم بمعظم العمل، فهو ينتظر الطلبات ويعالجها ويرسل المعلومات المطلوبة للزبون، وفي بعض التطبيقات يستطيع بعض المستخدمين تنفيذ تطبيقات معينة على آلة المخدّم ومعالجتها، كما في حالة الاتصال عن بعد (Telnet) وتطبيقات CGI (Common Gateway Interface).

وفيما يلي نعرض متطلبات تحقيق هذا المفهوم على شبكة إنترانت.

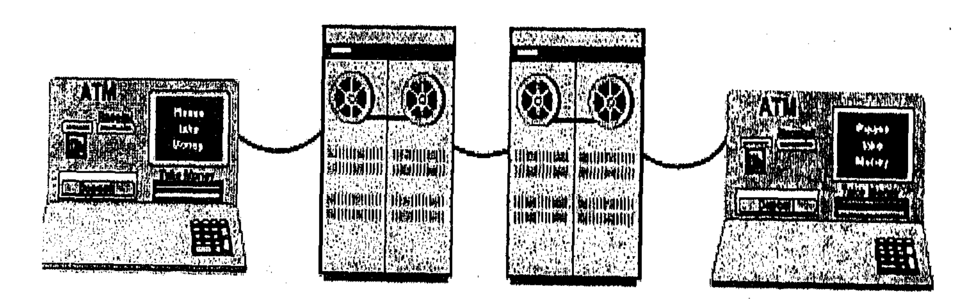
3-2-2 المخدّم

يمكن أن تستخدم مؤسسة ما أو مجموعة عمل معينة، مخدّماً أو أكثر وذلك حسب احتياجاتها. ولنبدأ بالمثال التالي: يستخدم أحد البنوك عدداً من المخدّمات كل منها خاص بأحد فروعه ؛ تعمل هذه المخدّمات على معالجة الطلبات المختلفة التي تصلها وفق أحد الخيارين التاليين:

الإجابة على الطلب وتحديث المعلومات المتعلقة به.

إرسال الطلب إلى المكان الصحيح.

فإذا كان لدينا طلب سحب مبلغ من أحد الحسابات، ولنفترض أن الطلب يأتي من فرع لا يملك فيه المستخدم حساباً، وذلك من خلال مناقلة لآلة الصرف الآلي (ATM Transaction)، يجب في هذه الحالة توجيه الطلب إلى المكان الصحيح، أي إلى الفرع الذي يحوي حساب المستخدم. في هذه الحالة يتصرف مخدّم آلة الصرف كزبون بينما يعمل مخدّم فرع المستخدم كمخدّم حيث يقوم بمعالجة الطلب وإجراء التغييرات اللازمة على الحساب، ثم تعاد المعلومات المطلوبة إلى آلة الصرف التي تقوم عندئذٍ بدور المخدّم بينما يكون الزبون هو المستخدم.



الشكل (3-4): آلة الصرف الآلي كمخدّم وزبون

لا توجد حدود لتطبيقات هذا النوع من التخاطب بين الزبون والمخدّم في عالم الأعمال، فأي نوع من المعطيات المطلوب الوصول إليها وتعديلها من قبل عدة مستخدمين يمكن أن يجري وفق نموذج زبون/مخدّم بكفاءة عالية.

البنية المادية للمخدّمات

قبل أن نبدأ بعرض الخيارات المتعلقة بالبنية المادية التي يمكن اللجوء إليها لتحديد مواصفات مخدّمات مؤسسة ما، يجب في البداية تحديد احتياجات المؤسسة الفعلية وهذا الأمر يستدعي تركيز الاهتمام في الأمور التالية:

1- الاستيعاب الأولي

من المعلوم أن الإنترانت تقدم لأي مؤسسة ـ سواء أكانت مؤسسة تعاونية أو تعليمية أو ما شابه ذلك ـ مركزاً للمعلومات لم يكن متوفراً من قبل، ومن ثم فإن التنبؤ بحجم استخدام الإنترانت من قبل المستخدمين في المؤسسة وتحديد القدرة الاستيعابية التي يجب أن توفّرها المخدّمات في الشركة هما من التحديات الصعبة التي تجب مواجهتها. ومن الأمور المساعدة في تحديد الاستيعاب المطلوب هو اختيار مجموعة من المستخدمين في مشروع تجريبي لتحديد مستواهم التقني في التعامل مع الإنترانت ومدى استخدامهم لها، ويجب أن نأخذ بعين الاعتبار مقدار حماسهم للمشروع والذي يلعب دوراً كبيراً ـ في بعض الأحيان ـ في تطوير مستوى قدراتهم التقنية. وفي كل الأحوال إذا كانت عملية تحقيق هذا المشروع التجريبي صعبة فيمكن الارتكاز على النقطتين اللاحقتين في تحديد نوعية المخدّمات المطلوبة في شبكة الإنترانت.

2- قابلية التطوير

إن قابلية التطوير هي من أهم العوامل في تحديد مواصفات المخدّمات العاملة على شبكة الإنترانت. وبما أن نجاح أي مشروع يتعلق بمدى استخدامه فإن هذا النجاح يجب أن يُتابع بتطوير في الخدمات التي تقدّمها المخدّمات. وبالنسبة للعديد من المخدّمات فإن تأمين بعض الموارد الإضافية يزيد من فاعليتها، مثل تطوير المعالج أو حجم القرص الصلب أو توسيع الذاكرة. وفي بعض المخدّمات يمكن زيادة الفاعلية بدون أي تغيير في البرمجيات، ومن المفضل استخدام مخدّمات تعمل ضمن حدود إمكانياتها الدنيا بدلاً من مخدّمات تعمل بطاقتها القصوى، مما يسمح بزيادة فاعلية أداء هذه

المخدّمات عند ازدياد حجم الاستخدام. فعلى سبيل المثال إذا كان المخدّم يعمل على نظام Windows 95 فسيبقى التطوير في البنية المادية محصوراً ضمن معالجات Pentium، أما في حالة Windows NT فيمكن استخدام معالجات مثل DEC Alpha بدون أي تغيير في البرمجيات.

3- *البنية الفعلية*

إن المخدّم الملائم للمؤسسة يجب أن يحقق نوعاً من التوافق مع الأنظمة الموجودة مسبقاً في الشركة، وكذلك مع المعرفة التقنية التي يمتلكها العاملون في الشركة. فعلى سبيل المثال إذا كانت الشركة تستخدم فعلياً سلسلةً من معالجات SPARC، فإن اختيار مخدّمات بمعالجات INTEL قد لا يكون الخيار الأفضل.

يمكن أن نناقش أيضاً في مجال البنية الفعلية عدم إغفال متطلبات الجاهزيّة الدائمة، فإذا كانت مخدّمات الشركة تعمل طوال 24 ساعة في اليوم عندها يكون من المستحسن استخدام مخدّمات تحقق وثوقية عالية في مجابهة الأعطال، كاستخدام تقنية RAID (Redundant Array of Inexpensive disks) لمواجهة الأخطار الناجمة عن تعطّل سواقات الأقراص الصلبة، وكذلك التقنيات المتوفرة في مواجهة الأعطال الناجمة عن التعطل في التيار الكهربائي. فإذا كانت الإنترانت تخدّم العديد من المستخدمين في نفس الوقت فإن تعطل أحد المخدّمات سيؤدي إلى تعطيل في أعمال المؤسسة، وقد يحدث أضراراً مادية كبيرة.

المخدّم الذي يدعم تقنية RAID يكون مخدّماً مزوّداً بمجموعة من الأقراص الصلبة التي تحمل نفس النسخة من المعلومات على كل منها، وعند أي تعديل في أحد الأقراص فإن هذا التعديل يجري على بقية الأقراص آلياً، بحيث إذا تعطل أحد الأقراص فإن المعلومات تظل محفوظة على الأقراص الأخرى.

الخيارات

إضافةً إلى النقاط السابقة فإن اختيار البنية المادية المناسبة لخدّمات الشبكة يجب أن يأخذ بعين الاعتبار الوظيفة الأساسية للمخدّم، وهي نقل المعلومات من أماكن تخزينها إلى الشبكة، ومن ثم يجب أن يملك المخدّم نظام دخل/خرج متماسكاً، فالعديد من سواقات الأقراص وبطاقات الشبكة مصممٌ للعمل على حواسيب عادية، وغير ملائم للعمل في بيئة تتطلب الكثير من عمليات الدخل والخرج المتنافسة، وهذا يعني أن نستخدم على سبيل المثال واجهة SCSI (Small Computer Systems Interface) بدلاً من واجهة IDE (Integrated Device Electronics)، فكلا الواجهتين كثيرة الاستخدام في البنى المادية للحواسيب، حيث تمثلان واجهة التخاطب بين المعالج والأجهزة الطرفية، ومن وجهة نظر الشبكات فإن استخدام واجهة SCSI يعني استخدام شبكة تحتوي على بعض العناصر "الذكية".

إن البنية المادية التقليدية للمخدّمات هي حواسيب كبيرة مثل SUN أو CRAY، أو حواسيب IBM متطورة أو حواسيب DEC. ولكن مع ظهور معالجات Pentium و Power-PC أصبح بالإمكان استخدام الحواسيب الشخصية كمخدّمات ولكن لاستخدامات محدودة، كمخدّمات وب أو مخدّمات للبريد الإلكتروني أو حتى مخدّمات FTP. ولكن بالنسبة لخدّمات Telnet ومخدّمات قواعد البيانات فنحن بحاجة إلى مخدّمات ذات قدرات أكبر، وفي الفقرة التالية سنناقش مختلف أنواع البنية المادية للمخدّمات ونعرض إيجابياتها وسلبياتها.

1- أجهزة Intel

يمكن أن يكون هذا المخدّم أي حاسوب شخصي بمعالج Intel متطوّر جرى إعداده كمخدّم بعد إعداد البرمجيات المطلوبة، أو قد يكون مصنّعاً خصيصاً ليعمل كمخدّم، وأغلب نظم التشغيل يمكن أن تعمل على هذا النوع بما فيها أنظمة Windows وكذلك UNIX و Solaris، وبسبب مكانة شركة Intel فستكون هذه الشركة أول من يدعم التقنيات الجديدة الممكن ظهورها في عالم المخدّمات.

الجانب السلبي في هذا النوع هو أن تعدد التراكيب الممكنة للعناصر الداخلية قد يجعل عملية تحديد مكان المشاكل عملية صعبة، فقد تتضارب العناصر المختلفة فيما بينها.

يمكن مثلاً أن تسبب مجموعة من العناصر مثل BIOS وسواقة الأقراص المرنة وبطاقة الشبكة مشاكل تضارب تؤدي إلى تعطّل المخدّم، وللتخلص من هذه السلبية يجب اختيار هذه العناصر من شركة مصنّعة واحدة تكفل عمل هذه المجموعة دونّ تضارب.

2- أجهزة *SPARC*

تُصنّع مخدّمات SPARC من قبل شركات SGI, SUN إضافةً إلى شركات أخرى ؛ ومعالج SPARC مصمّم خصيصاً للمعالجة السريعة للطلبات المتنافسة على مخدّم يتلقى ضغطاً شديداً في شبكة إنترانت. وقد استطاعت شركة SUN أن تكسب مكانة تسويقية من خلال إضافة العديد من المزايا القيّمة إلى منتجها، كتزويد المخدّم بالبرمجيات اللازمة لبناء وتشغيل وإدارة مواقع الوب وذلك في سلسلة مخدّمات Netra، والعديد من الشركات تحذو حذوها الآن.

3- أجهزة *Macintosh*

تحتل أجهزة ماكينتوش مكانة قوية في تسويق مخدّمات الوب بفضل واجهتها التخاطبية السهلة، وسهولة إعداد تطبيقات TCP/IP إضافةً إلى أدوات إدارة مواقع الوب، ولكنها لا تستطيع أن تدعم نفس العدد من المستخدمين مقارنةً بالمعالجات الأخرى.

برمجيات المخدّمات

يمكن وضع العديد من المخدّمات على حاسوب واحد، أي يمكن جمع مخدّم وب مع مخدّم FTP ومخدّم بريد إلكتروني ومخدّم لقواعد المعطيات على جهاز واحد. ويستمع كل من هذه المخدّمات للاستفسارات الخاصة به ويجيب عليها. تحتاج بعض المخدّمات إلى جزء صغير من الذاكرة مثل

مخدّمات FTP ومخدّمات البريد الإلكتروني، ويحتاج البعض الآخر مثل مخدّمات الوب وقواعد المعطيات إلى حجوم أكبر من الذاكرة، حيث يمكن استخدام حاسوب Pentium مع ذاكرة 32MB RAM كمخدّم للوب، بينما يجب استخدام ذاكرة 128MB RAM فيما لو أردنا تشغيل أكثر من مخدّم على هذا الحاسوب، وذلك حسب عدد المستخدمين الذين قد يطلبون خدمة معينة في الوقت نفسه، أو حسب عدد الطلبات التي تجب معالجتها في آن واحد.

نظم تشغيل المخدّمات

تأتي أهمية اختيار نظام التشغيل بالنسبة للمخدّم من أنه يمثل النظام الوسيط بين البنية المادية وبرمجيات المخدّم، وبما أن نظام التشغيل هو مفتاح اختيار المخدّم فإن الخيار الجيد سيؤثر حتماً على أداء المخدّم، وذلك للعديد من الأسباب، فنظام التشغيل يحوي جميع الأدوات اللازمة لتهيئة المخدّم وإدارته، وفي العديد من الحالات فإن الخيارات قد تصبح محدودة بعد اختيار البنية المادية، كما أن اختيار البنية المادية بالنسبة لبعض المخدّمات يعتمد على نوعية نظام التشغيل.

فإذا كان المخدّم مثلاً يستخدم معالج SUN، فإننا سنكون مضطرّين لاستخدام نظام تشغيل Solaris وهو النسخة الخاصة بـ SUN من النظام UNIX. في حين إذا كانت البنية المادية للمخدّم تستخدم معالج Pentium فهناك العديد من الخيارات، والجدول (3-1) يعرض أنظمة التشغيل والمعالجات التي يمكن أن تعمل عليها هذه الأنظمة.

نظام التشغيل	Pentium	Macintosh	SUN	DEC
Windows NT	*			
Windows 3.1	*			
Windows 95	*			
Solaris	*		*	
UNIX	*	*	*	*

Linux	*	*		
MacOS		*		
SUN OS			*	

الجدول (3-1): توافق نظم التشغيل والمعالجات

يؤثّر اختيار نظام التشغيل في مستقبل الإنترانت، إذ قد يزداد حجم الشبكة بحيث لا يستطيع نظام تشغيل مثل Windows 95 أو MacOS السيطرة عليها، وعندها يجب تحويل جميع التطبيقات للعمل ضمن بيئة UNIX وهذا ليس بالعمل السهل.

ونناقش فيما يلي بعض أنظمة التشغيل التي يمكن اختيارها:

1- *Solaris*

طُوّر هذا النظام من قبل شركة Sun Microsystems كبديل لنظام SunOS وذلك ليعمل على معالج SPARC الذي تطوره هذه الشركة أيضاً. يعتمد هذا المعالج تقنية RISC وهو قادر على القيام بالعديد من المهام بنفس الوقت، وتستخدمه العديد من الجامعات والمؤسسات الكبرى. ويحتل نظام التشغيل Solaris المكانة التجارية الأكبر، وذلك يعود إلى أنه نسخة UNIX الأكثر شعبية، إضافةً إلى الاهتمام الذي تبديه شركة Sun في دعم تجهيزات الإنترنت، حيث قامت هذه الشركة بعزل المجموعة التي طوّرت نظام التشغيل وأصبحت تعمل تحت اسم Sunsoft ؛ وقد طورت Sunsoft نظام Solaris ليعمل على معالجات Intel إلاّ أنه لم يلاق إقبالاً كبيراً بسبب صعوبة تثبيته وتهيئته.

2- *SCO UNIX و BSD UNIX*

تعتبر هاتان النسختان من نظام التشغيل UNIX أكثرَ النسخات التجارية التي تعمل على معالجات Intel شعبية، وقد بدأ نظام Santa Cruz SCO UNIX Operating System كنظام تشغيل Xenix، ومن ثم طوّر في الإصدارات المسماة Open Systems و Open Server. تملك هذه الإصدارات واجهة

تخاطب بيانية بدلاً من واجهات الأوامر النصيّة التي لازالت تشكّل نواة نظام UNIX. وتدعم هذه الأنظمة تعدّد المستخدمين في شبكات الإنترانت الصغيرة والكبيرة على السواء، إذ يمكن تشغيل مخدّم وب ومخدّم بريد إلكتروني بفاعلية في هذه الأنظمة لتخديم 20 مستخدماً مثلاً على معالجات 386 بفرض أننا نستخدم ذاكرة من حجم 12 MB أو 16 MB. وإذا كانت الإنترانت كبيرة الحجم فيمكن تخديم 100 مستخدم أو أكثر، ومن ثم يمكن الاستغناء عن التكاليف الباهظة في البنية المادية والبرمجيات اللازمة لاستخدام المعالجات القوية مثل SUN أو SGI، والحصول على أداء لمعالجات Pentium في تشغيل أنظمة UNIX أفضل من أدائها في تشغيل أنظمة Windows 95 أو Windows NT. ويفضّل العديد من مدراء الأنظمة استخدام أنظمة التشغيل UNIX لأنها مزودة بالكثير من تطبيقات الإنترانت، غير المتوفرة في الأنظمة الأخرى مثل Windows أو Macintosh، كتعليمة Finger ومخدمات البريد الإلكتروني التي تُعتبر معيارية في أنظمة UNIX. كما تزود أنظمة UNIX المستخدمين بحسابات عليه، مما يعني إمكان استخدام مساحة معينة من القرص الصلب للمخدّم حيث يمكن مثلاً تخزين البريد الإلكتروني على المخدّم، والسماح للمستخدمين بالنفاذ المباشر إليه. ومن الأمور الأخرى التي تميز نظام UNIX أنه يعمل على أي بنية مادية تقريباً، الأمر الذي يزيد من قابليته للتطور.

أمّا بالنسبة لنظام BSD UNIX فإنه يلاقي إقبالاً متزايداً منذ إصداره الأول عام 1993، حيث كان قد طُوّر في شركة Berkley Software Design على أساس تعديلات وتغييرات على نظام UNIX قام بها مجموعة من الطلاب والعاملين في جامعة California. وتتركز أغلب التعديلات في مفسّر الأوامر Shell وبعض الوظائف، وقد لا نلاحظ الفرق بين مختلف إصدارات UNIX إلاّ إذا كانت لدينا اهتمامات برمجية عميقة. كما توجه هذا النظام نحو سوق الإنترانت والإنترنت، ويستخدم حالياً في العديد من المواقع الكبيرة على الإنترانت مثل موقع Adobe وموقع Intel، ويملك بعض البوابات البرمجية التي تسمح لخدّماته بالتخاطب بسهولة مع المواقع التي تشغل Novell Netware.

Linux -3

بُني نظام Linux من قبل Linus Torvalds الذي كان يعمل على إيجاد نسخة من نظام UNIX أكثر سهولة في التهيئة وتعمل على معالجات X86 وتكون علاوة على ذلك مجانية، ولذلك بني هذا النظام على مبادئ نظام UNIX ولا يستطيع العديد من المستخدمين التمييز بينهما. وقد جرى تطوير هذا النظام واختباره نتيجة جهود العديد من التطوعين، ولا توجد أي شركة مسؤولة عنه، حيث يمكن لأي شخص أن يعدّل في هذا النظام. وبسبب كون هذا النظام مجانياً لم يجرِ تجميعه وإضافة التعليمات المساعدة لتثبيته إلا مؤخراً، وذلك من قبل عدد من الشركات التي تقوم بهذه المهمة وتوزع النظام مجاناً. ويُعزى نجاح هذا النظام إلى مرونته المدهشة، فبإمكان المستخدمين تغيير أي ميزة من ميزاته وتخصيصها لتعكس الاهتمامات الشخصية، فإذا توفرت المعرفة الجيدة بهذا النظام وأردنا بناء موقع وب بكلفة قليلة فإن اختياره كنظام تشغيل سيكون الخيار الأمثل.

Windows NT -4

بدأت شركة Microsoft بتطوير هذا النظام في أواخر الثمانينيات، عندما اتضح لها بأن نظام OS/2 لن يكون نظام تشغيل التسعينيات بسبب ضعف هذا الأخير في دعم البنى المادية المختلفة، إذ كان قد بُني خصيصاً لمعالجات Intel. وفي عام 1992 أعلنت شركة Microsoft عن البدء بمشروع بناء نظام تشغيل غرضي التوجه يعمل على مختلف البنى المادية، وفي عام 1993 أصدرت النسخة الأولى من نظام Windows NT 3.1.

عند ظهور الإصدارات الأولى لهذا النظام لم تحقق شركة Microsoft آمالها في أن يكون نظام التشغيل الأول والذي سيضع حداً لأنظمة التشغيل الأخرى، ولكنه في إصداراته الأخيرة اعتبر نظاماً متماسكاً ومستقراً، وبدأ باستقطاب اهتمام وسائل الإعلام وسوق البرمجيات. ودعم نظام Windows NT المعالج Alpha من شركة DEC، مما وسع عددّ الخيارات المطروحة في البنى المادية عند اختيار Windows NT، وساهم في جعل هذا النظام في المقدمة بين نظم التشغيل المختلفة. وكما هي الحال في نظام UNIX فإن Windows NT يشغّل الإجرائيات البرمجية وفق أحد نمطين: نمط المستخدم (User

Mode) ونمط النظام (Kernel Mode)، وهذا التمييز بين النمطين جعل النظام أكثر استقراراً، فأي إجراء يعمل في نمط المستخدم لا يمكن له أن يوقف عمل النظام.

وابتداءً من النسخة Windows NT 4.0 فقد أصدرت Micosoft مخدّم معلومات الإنترنت (Internet Information Server <IIS>) الذي يتكوّن من مجموعة برمجيات تضمّ مخدّمات مثل مخدّم الوب ومخدّم نقل الملفات FTP ومخدّم Gopher.

وقد يناسب هذا النظام العديد من المؤسسات المتوسطة الحجم، والتي لا ترى ضرورة في توظيف مختصين بنظام UNIX ضمن طاقمها من أجل الاهتمام بآلة واحدة.

5- *OS/2*

بدأ هذا النظام بآمال وتوقعات كبيرة، حيث قامت شركتا IBM و Microsoft بإصدار هذا النظام في عام 1987 ليكون خليفة لنظام MS-DOS، وخلال سنوات قليلة تخلّت شركة Microsoft عن المشاركة في تطوير النظام الذي تولت شركة IBM مهمة تطويره وتسويقه. وفي أوائل التسعينيات طُوّر هذا النظام ليعمل ضمن بنية مادية محددة وليدعم مفهوم زبون/مخدّم، وبدأ بعض مطوّري البرمجيات باستخدام بعض مزايا OS/2 لتثبيت أقدامهم في السوق التجاري المتنامي لبرمجيات زبون/مخدّم. من ثم أصدرت شركة IBM نظام التشغيل OS/2 Warp، وهو نظام تشغيل قوي يتمتع بالعديد من المزايا مثل دعم الشبكات وتوفير مخدّم للأسماء، وعلى الرغم من أن هذا النظام لم يلاق نجاحاً تجارياً إلا أنه يبقى نظاماً متماسكاً.

6- *MacOS*

في أواسط الثمانينيات طوّرت شركة Apple نظام تشغيل MacOS وركّزت على أن يكون سهل الاستخدام، فقدّم هذا النظام أسهل واجهة تخاطبية بين أنظمة التشغيل المتوفرة في ذلك الوقت. ويقدّم نظام Mac OS كمخدّم وب العديد من المزايا الجيدة، بما فيها أدوات لتنظيم وإدارة الوب سهلة

التهيئة. والمشكلة الوحيدة في استخدام هذا النظام كنظام تشغيل لمخدّم إنترنت هي في قدرته الاستيعابية، حيث لا يستطيع - كمخدّم - أن يتعامل بكفاءة مع أكثر من 50 مستخدماً في الوقت نفسه، ولكن يمكن استخدامه في مشروع تجريبي لشبكة إنترانت في مؤسسة متآلفة مع هذا النظام.

7- أنظمة التشغيل الأخرى

هناك أنظمة تشغيل أخرى يمكن أن تدعم مخدّمات الإنترانت، ومن الممكن اختيار بعض هذه الأنظمة إذا كانت تمثّل البيئة الوحيدة الملائمة للمخدّم الذي سيعمل عليها. على سبيل المثال قامت شركة Novell بإصدار العديد من مخدّمات الوب التي تسمح بدعم موقع وب على نظام Novell NetWare. ويمكن اختيار هذا النظام في شبكة إنترانت لشركة تستثمر مخدّمات Novell وتملك شبكة تحتية تعمل وفق البروتوكول IPX.

في النهاية نذكّر أنه يمكن تبنّي بعض الخيارات اعتماداً على خبرة العاملين في الشركة أو لأن الأنظمة موجودة مسبقاً، مثل أنظمة AIX و نسخة UNIX من IBM التي تعمل على RS/6000 من شركة IBM، أو HP/UX وUNIX من Hewelett Packard التي تعمل على HP9000.

3-2-3 الزبون

نناقش فيما يلي الخيارات المكنة في تجهيزات المستخدمين ماديةً كانت أم برمجية، كما سنوضح تأثير هذه الخيارات على تطبيقات الخدّمات والتوصيل.

التجهيزات المادية

على الرغم من أن الجزء الأساسي في متطلبات المستخدمين هو البرمجيات، يبقى مهماً أن نقارن سلبيات وإيجابيات البنى المادية المختلفة المكن اعتمادها في شبكة الإنترانت (خصوصاً في حالة عدم وجود بنية تحتية مسبقة). ففي حين تعتبر عملية ربط المستخدمين من أكبر التحديات في بناء

الإنترانت، يمكن أن يكون اختيار التجهيزات المادية الملائمة ونظم التشغيل العاملة عليها من أهم العوامل المبسّطة لهذه التحديات.

وفيما يلي سنقوم باستعراض بعض الخيارات المكنة.

1- حواسيب ماكينتوش

على الرغم من شعبيتها المنخفضة نوعاً ما في عالم الأعمال، إلا أنها معتمَدة على نحو كبير في المؤسسات التعليمية، حيث نشأت أولى التطبيقات المعتمدة على بروتوكولات TCP/IP، وكذلك تطبيقات زبون/مخدِّم، كما أن العديد من التطبيقات المعدّة لمستخدمي الشبكات أعدّت أساساً (وأحياناً حصراً) من أجل بيئة الماكينتوش.

ولهذه الحواسيب أنظمة التشغيل الخاصة بها، مثل نظام MacOS 7.0 المزود بخدمات TCP/IP مستقرةٍ وسهلةِ الاستخدام، كما أن هذا النظام يقدم تقريباً كافة تقنيات الوصل والتشغيل الفوري (Plug and Play) ويتفوق على الحواسيب الشخصية المتوافقة مع IBM في هذا المجال.

إن أسعار الماكينتوش حالياً أعلى بقليل من أسعار الحواسيب الشخصية المتوافقة مع IBM (PCs)، ولكنها تقترب من المعايير العالمية لأسعار الحواسيب الشخصية كنتيجة لمحاولات شركة Apple لرفع مكانتها التجارية.

ومما لاشك فيه أن الماكينتوش هو من أبسط الأجهزة من حيث إمكانية وصلها بالإنترانت أو الإنترنت، لأن أغلب نماذجه مزودة بمآخذ للوصل مع الشبكة والموديمات، حيث يمكن لأي مستخدم شبك مأخذ الوديم أو الشبكة وبعد اتباع بعض التعليمات يصبح على اتصال في زمن قصير.

ويسهل الماكينتوش عملية إضافة الأجهزة مثل الوديمات و السواقات الإضافية و أجهزة SCSI ومكبرات الصوت مادامت هذه الأجهزة خارجية، إذ إن إضافة الذواكر الداخلية أو كروت العرض الفيديوي أو كروت الصوت هي عملية أكثر صعوبة مقارنةً مع الحواسيب الشخصية PC.

ويتفوق الماكينتوش على الحواسيب الشخصية PC بالقدرات الصوتية، ويبدو أنه يسيطر على مكاملة الصوت والصورة مع نظام التشغيل، على الرغم من أن نوعية الصوت والصورة ليست أفضل منها على أي حاسوب PC متطور.

من مساوئ الاعتماد على الماكينتوش في الإنترانت قلة البرمجيات التجارية المتوافقة معه، ففي معظم مراكز البيع المتخصصة بالحواسيب يكون الجناح الخاص بالماكينتوش منعزلاً في زاوية بعيدة. كما أن الشركة المتبنية للماكينتوش وهي Apple Computers تعاني من مشاكل مالية وإدارية مؤخراً، ويبقى مستقبلها غير أكيد، ولكن من المؤشرات الجيدة أن هذه الشركة قامت بالترخيص لبعض الشركات بإنتاج نظامها ومعالجها، ولم يعد المستخدمون بحاجة للاعتماد على مصدر واحد لأنظمة التشغيل أو للقطع الإلكترونية الخاصة بالماكينتوش، ومن غير المحتمل زوال الماكينتوش في أي وقت حالياً، ولكن إيجاد التطبيقات البرمجية العاملة على الماكينتوش لن يصبح أسهل.

إن نظام التشغيل MacOS نظام مستقر، ويعمل جيداً على 8MB RAM، كما يسمح بتعدد المهمات ويتفوق بهذا الأمر على أنظمة Windows 3.x و Windows 95 ولكنه ليس بجودة نظامي Linux أو Windows NT.

2- *الحواسيب المتوافقة مع IBM*

هذه الحواسيب المعروفة باسم الحواسيب الشخصية PCs، هي الأكثر شعبية في عالم الأعمال حتى الآن، كما يمكن القول إنها الأكثر شعبية بين مستخدمي الشبكات، وهذا بسبب توفر العديد من نظم التشغيل العاملة عليها وكلها قادرة على التعامل مع بروتوكولات TCP/IP.

ولكن هذا لا يعني أن هذه الحواسيب خالية من العيوب. فحتى عام 1995 كان من غير المألوف أن تُباع حواسيب PC مع إمكانيات صوتية، وحتى الآن لا يمتلك العديد من مستخدمي الشبكات إمكانيات صوت وصورة عالية، وهناك العديد من الصعوبات لتوصيل المستخدمين البعيدين الذين يحاولون النفاذ إلى الشبكة باستخدام موديم، على الرغم من أن العديد من أنظمة التشغيل تسعى

لتحقيق هذه العملية بسهولة، فمعالجة المشاكل الممكن حدوثها عند محاولة النفاذ من أنظمة Windows 3.x و Windows 95 إلى شبكة إنترانت باستخدام موديم عملية صعبة، حيث يوجد العديد من العوامل التي تصعب عملية وصل المستخدمين البعيدين إلى الشبكة، منها ما يتعلق بالبنية المادية، أو ببرمجيات الشبكة، أو بالتهيئة الصحيحة لأنظمة التشغيل.

إن تطوير البنية الداخلية للحواسيب المتوافقة مع IBM أكثر سهولة من تطوير بنية الماكينتوش، ويؤدي التنافس القوي في سوق الحواسيب فيما يخص البنية المادية و البرمجيات و ملحقات الحاسوب إلى انخفاض الأسعار مقارنة مع أسعار الماكينتوش.

أنظمة تشغيل الحواسيب الشخصية

هناك العديد من أنظمة التشغيل العاملة على الحواسيب المتوافقة مع IBM، بعضها أكثر تخصصاً من الأخرى، ويمتلك بعضها بعض الميزات القوية فيما يخص تطبيقات TCP/IP. وعموماً فإن اختيار نظام التشغيل يجب أن يتوافق مع التطبيقات التي يرغب المستخدم في العمل عليها، فالمستخدمون الذين تقتضي أعمالهم المعالجة النصية والحسابية قد يختارون نظام Windows 95 بسبب قوة التطبيقات المتوفرة ضمن هذه البيئة فيما يخص الأمور السابقة، أما المستخدمين الذين يقضون معظم الوقت في العمل على شبكة الإنترانت أو الإنترنت فإن نظام Linux يكون أكثر مرونة واستقراراً بالنسبة لهم على الرغم من أن تطبيقات المعالجة النصية والحسابية المتوفرة ضمن بيئته ليست على نفس الدرجة من القوة والغنى.

Windows 3.1 –1

على الرغم من أن Windows 3.1 كانت بلا شك من أكثر أنظمة التشغيل انتشاراً في المؤسسات فقد أصبحت قديمة ضمن مقاييس البرمجيات الحديثة (مع الأخذ بعين الاعتبار الصعوبات التي قد تعترضنا عند ربط موديم أو الربط مع الشبكة المحلية)، إلا أن العديد من البرمجيات والخدمات

المساندة متوفر ضمن هذا النظام. وهي بيئة قليلة الثبات وغير مستقرة، فعند حدوث أي تشويش تتوقف عن العمل مع إظهار الرسالة الشهيرة "General Protection Fault".

تعمل Windows 3.1 جيداً على معالجات 386 أو 486 مع ذاكرة 4MB RAM، وهي نظام تشغيل مبني على أساس 16 bit، ولكنها لا تدعم تعدد المهمات على نحوٍ حقيقي، بمعنى أنه لا يمكن أن تقوم بأكثر من عملية في نفس الوقت بفعالية تامة.

Windows NT -2

نظام تشغيل يعمل على أساس 32Bit ويحتاج إلى 16MB RAM على الأقل ليعمل بكفاءة. ظهر منذ عام 1993 ويعتبر أساس نظام Windows 95، يدعم تعدد المهام دعماً ممتازاً، ويستطيع تشغيل العديد من برمجيات Windows 95. من مساوئه صعوبة تهيئته عند التعامل مع الشبكات والنقص في الدعم التقني (المتوفر بسعر عالٍ)، كما أن تكلفته عالية جداً ويتطلب إدارة نظام خبيرة، وحالياً يعتبر من الأنظمة المفضلة لدى مديري الشبكات والمستخدمين المتقدمين، ويبدو أن شركة Microsoft تسعى لاستبداله بنظام Windows 95 حيث أن نظام Windows NT 4.0 الذي ظهر في عام 1996 يمتلك واجهة Windows 95 ومزايا Windows NT.

Windows 95 -3

من أكثر أنظمة التشغيل انتشاراً بين مستخدمي شبكات TCP/IP الحالية، وهو مبنيٌ على أساس 32 Bit ويدعم التعدد بالمهمات دعماً معقولاً، وقابلٌ للتعامل بسهولة مع شبكات TCP/IP والشبكات المحلية، ولكنها صعبة التهيئة نوعاً ما للنفاذ إلى الشبكة عبر الهاتف مقارنة مع النفاذ المباشر. ويواجه العديد من مزوّدي خدمة الإنترنت ISP مشكلة تهيئة توصيل المستخدمين باستخدام الموديم في حالة شبكات غير شبكات Microsoft.

وعلى الرغم من أن شركة Microsoft تصرح بأن نظام Windows 95 يستطيع العمل على حاسوب بذاكرة 8MB RAM إلى أنها تبقى بطيئة بأقل من 12MB RAM.

4- OS/2

قليل الاستخدام، يعمل على أساس 32 Bit ويحتاج إلى 8MB RAM ليعمل جيداً، كما أنه يدعم تعدد المهمات دعماً ممتازاً. صعب التهيئة، لكنه مزود بخدمات TCP/IP مستقرة، ويمكن أن يعمل مع العديد من مزودي خدمة الإنترنت عندما تجري تهيئته على نحوٍ صحيح، له بريده الإلكتروني الخاص، وخدمات FTP و Telnet، وكذلك مستعرض لصفحات الوب، ويعمل العديد من تطبيقات Windows 3.x و Windows 95 عليه بصورةٍ جيدة (إلا أنها بطيئة)، لكن هذا النظام تنقصه البرمجيات المساندة.

5- Linux

نظام Linux هو نظام تشغيل غير تجاري متعدد المزايا، يعمل بكفاءة على حواسيب 486 مع ذاكرة 8MB RAM، وهو مبني على أساس 32bit ويدعم تعدد المهام دعماً حقيقياً، كما أنه الأسرع والأكثر قابلية للتخصيص بين الأنظمة المتوفرة، يمكن الحصول عليه مع معلومات كاملة تكفي لعملية التثبيت من صفحة Linux في الإنترنت على العنوان التالي: http//www.linux.org.

6- أنظمة التشغيل الأخرى

هناك العديد من أنظمة التشغيل الممكن استخدامها والتي تعمل على العديد من البنى المادية مثل آلات Amiga القديمة، أو محطات SUN أو SPARC أو محطات Silicon Graphics. وفي كل الأحوال، إذا لم يكن مدير النظام على دراية كاملة بالتجهيزات الممكن اعتمادها فليس من الحكمة اختيار تجهيزات غير منتشرة الاستعمال.

البرمجيات

تتفاعل برمجيات المستخدمين (والتي نسميها الزبون ضمن مفهوم زبون/مخدّم) مـع المخدّمـات لإتمـام معاملات TCP/IP، وكل البرمجيات التي سنناقشها تترجم طلبات المستخدم و دخلـه إلى لغـة معينـة يستطيع المخدم فهمها والتواصل مع المسـتخدم عـبر بروتوكـولات TCP/IP، ولكـلٍّ مـن هـذه اللغـات بروتوكـول معـين يحكمـها ويجـري تصنيفـه في الطبقـة السـابعة (طبقـة التطبيقـات) ضمـن نمـوذج ISO/OSI.

1- *المستعرضات (Browsers)*

عند وجود مخدّم وب على الإنـترانت فالمسـتعرضات ضروريـة للمسـتخدمين. وظيفـة المسـتعرض هـي إرسال ملف مـن الطلبـات إلى مخـدّم الـوب وعـرض المعلومـات القادمـة مـن المخـدّم، وعمومـاً يمكـن للمستعرضات عرض المعلومات على شكل نصـوص أو صـور للمسـتخدمين، وبعضـها يسـتطيع عـرض المعلومات الصوتية أو الصور وأنواع الملفات الأخرى، كما يمكن للعديد من المستعرضات إعـادة إرسـال المعلومات إلى المخـدّم باسـتخدام الأشـكال الضمنيـة (Embedded Forms)، وتسـتطيع المسـتعرضات الحاليـة تشـغيل تطبيقـات معينـة مثـل تطبيقـات JAVA أو ActiveX، والـبروتوكول المسـتخدم في التخاطب بين مخدّم الوب والمستعرض هو بروتوكول HTTP (HyperText Transfer Protocol).

مستعرض Netscape

ما يزال مستعرض الصفحات Netscape من أكثر تطبيقات TCP/IP شعبية، وهو متوفر ضمـن العديـد من البيئات مثل MacOS و Windows 95 و Windows NT والعديـد مـن بيئـات UNIX وكذلـك Linux. يعمل هذا المستعرض جيداً على 8MB RAM، وبما أنه يتضمن خدمات نقل الملفات والـبريد الإلكتروني وقراءة الدوريات ضمن المستعرض فهو يتطلب عـدداً أقـل مـن التطبيقـات العاملـة في نفـس الوقت في ذاكرة حاسوب المستخدم. ويمكن الحصول على النسخ التجريبية من هذا المسـتعرض (Beta Versions) مجاناً.

يدعم هذا المستعرض لغة JAVA الخاصة بشركة SUN، وبالتالي يستطيع تنفيذ التطبيقات المكتوبة بهذه اللغة ضمن المستعرض، مما يعني أنه بغض النظر عن نظام التشغيل الذي يستخدمه المستخدم فإن المستعرض سينفّذ التطبيق تنفيذاً مماثلاً أياً كان نظام التشغيل.

مستعرض Internet Explorer

يُعتبر هذا المستعرض ردّ شركة Microsoft على مستعرض Netscape، فهو يملك العديد من مزايا Netscape، كما أنه يأتي مجاناً مع نظام Windows 98، ويعمل بكفاءة على 12MB RAM، لكن هناك بعض العوامل التي تجعل من مستعرض Netscape المستعرض الأفضل وفق أغلب المقاييس، فهو سريع، وله العديد من المزايا، لكن Explorer يأخذ مكانه شيئاً فشيئاً. ومن غير المؤكد معرفة أي المستعرضين سيسيطر على السوق، فعلى الرغم من أن Explorer يستمد قوته من شركة Microsoft إلا أن بعض المستخدمين يتوقعون زواله كما زال استخدام أشرطة التخزين المغناطيسية.

مستعرض نظام OS/2

يأتي هذا المستعرض مجاناً مع نظام OS/2، ويعمل بكفاءة على 8MB RAM، ومن الممكن مقارنته بالمستعرض Netscape أو المستعرض Explorer، لكنه لا يعمل إلا ضمن بيئة OS/2، كما أنه المستعرض الوحيد ضمن هذه البيئة، أي أن الخيار محدود في هذه الحالة.

مستعرض Mosaic

من شركة NCSA، وهو مستعرض كامل المزايا نسبياً، وغني بما فيه الكفاية لتغطية معظم الميزات الأساسية ؛ يعمل جيداً على 4MB RAM، وهو متوفر على الإنترنت ويكلف نصف تكلفة مستعرض Netscape، وعلى الرغم من أن Netscape يقدم مزايا أكثر من Mosaic إلا أن بعض المستخدمين قد لا يحتاجون إلى هذه المزايا الإضافية، ومن ثم فإن اختيار Mosaic قد يكون مناسباً.

2- برمجيات البريد الإلكتروني

إن أكثر الأجزاء أهمية في برمجيات المستخدمين هي برمجيات البريد الإلكتروني، فلقد أثبت البريد الإلكتروني نفسه كتطبيق ضروري في معظم بيئات العمل. وتختلف برمجيات البريد الإلكتروني المتوفرة حالياً في مقدرات الواجهة التخاطبية فقط، ويتم تبادل البريد الإلكتروني باستخدام بروتوكول SMTP حيث يحدد هذا البروتوكول صيغة عامة لإرسال الرسائل والملفات، وتستخدم أغلب تطبيقات البريد الإلكتروني القليل من موارد نظام حاسوب المستخدم، وتعمل بعض التطبيقات على حاسوب المخدّم. تعمل المخدمات الحالية وفقاً للبروتوكول POP3 (Post Office Protocol 3)، حيث يحتفظ مخدّم البريد بالبريد ضمن علبة بريد ليُرسله إلى المستخدم، أو يمكن أن يكتفي المستخدم بقراءته من المخدّم باستخدام أداة خاصة تدعى Pine يمكن تنفيذها من خلال الأداة Telnet.

هناك بروتوكول آخر للبريد الإلكتروني لا يزال حديثاً نوعاً ما، وهو IMAP (Interactive Mail Access Protocol) ؛ يسمح هذا البروتوكول بمعالجة رسائل البريد ضمن مجلد بعيد على المخدّم، ففي حين يستطيع المستخدم الوصول إلى علبة البريد للقراءة فقط باستخدام البروتوكول POP3، فإنه وباستخدام البروتوكول IMAP يستطيع أن يعالج بريده على المخدم من خلال بيئة تخاطب بيانية يمكن من خلالها القيام بعمليات التحرير من نسخ ولصق على مستخدمين آخرين، كما أن تخزين البريد يكون على المخدّم بدلاً من تخزينه على حاسوب المستخدم.

Eudora

أكثر برمجيات البريد الإلكتروني شيوعاً، يمتاز بمرونته ويمتلك العديد من المزايا، وهو متوفر ضمن بيئة ماكينتوش والعديد من بيئات Windows.

Netscape

كما ذكرنا فإن Netscape هو عبارة عن مستعرض مزود بقارئ للبريد الإلكتروني، ولكنه ليس بغنى Eudora من حيث الميزات، ولكنه يقدم الميزات الأساسية مثل كتابة الرسالة وتخزينها وكذلك دفتر العناوين، كما يقوم بفرز الرسائل وضغط حجم علبة البريد، ويمتاز بتوفيره في موارد النظام خصوصاً

عندها يعمل مع المستعرض في نفس الوقت، وكما ذكرنا فإن مستعرض Netscape متوفر ضمن العديد من نظم التشغيل.

SPRY

من تطبيقات البريد الإلكتروني الجيدة، وهو سهل التهيئة وسريع في نقل الرسائل، ويملك عدداً من مزايا Eudora ولكنه يعمل فقط مع الإنترنت ؛ إحدى ميزاته القوية هي قدرته على عرض علبة البريد من بعيد، بمعنى أنه بالإمكان حذف الرسائل غير المرغوب فيها بدون الحاجة إلى استقدامها إلى حاسوب المستخدم، وهو متوفر ضمن بيئات Windows 9x فقط.

Pine

لا يعتبر Pine كتطبيق بريد إلكتروني حقيقي، فهو عملياً برنامجٌ يعمل على المخدّم ويتوافق معيارياً مع العديد من المخدّمات ضمن بيئة UNIX، وله العديد من مزايا برامج البريد الإلكتروني التي تعمل على حاسوب المستخدم، مثل دفتر العناوين، وأدوات للبحث، وإمكانية إلحاق المستندات بالرسائل، ويتميز بكونه مجانياً ويسمح للمستخدمين بالوصول إلى بريدهم من أي مكان تقريباً.

3- برمجيات نقل الملفات

إن بروتوكول نقل الملفات FTP يشكّل طريقةً لنقل الملفات من المخدّم إلى الزبون أو العكس، وكما في حالة البريد الإلكتروني فإن نقل الملفات يجري عبر بروتوكولات TCP/IP، ولا يوجد أي فرق بين تطبيقات نقل الملفات البيانية وتطبيقات نقل الملفات من خلال الأوامر من ناحية المزايا التي يقدمها كل منهما، وتستخدم تطبيقات نقل الملفات جزءاً صغيراً من موارد النظام.

CuteFtp

هو تطبيق مجاني ويمكن الحصول عليه من الإنترنت، وله العديد من المزايا وهو مستخدم استخداماً كبيراً، ويملك واجهة بيانية بسيطة تشابه تطبيق مدير الملفات، بحيث يعرض في نافذته الأساسية

نظام الملفات البعيد في جهة ونظام الملفات المحلي في جهة أخرى. يتوفر هـذا التطبيـق ضمـن بيئـات Windows 3.x و Windows 9x ، ولكنه غير متوفر حتى الآن على حواسيب الماكينتوش.

Fetch

يعمل هذا التطبيق على حواسيب الماكينتوش فقط، ويملك العديد من المزايا، وهو التطبيق المفضل على الماكينتوش، وهناك نسخة مجانية جزئية لهـذا التطبيـق علـى الإنـترنت، ويملـك واجهـة تخاطبيـة مشـابهة لواجهـة التطبيـق السـابق، وإحـدى أهـم مزايـاه هـي قدرتـه علـى نقـل المجلـدات بكـامل محتوياتها.

تطبيقات نقل الملفات الأوامرية (Command Line FTP)

يقدم كل من Windows 95 و Windows NT وجميع أنظمة التشغيل UNIX تطبيقات نقـل الملفـات الأوامرية، حيث تجري عملية النقل من خلال كتابة العديد من الأوامر.

Telnet -4

يستخدم هذا التطبيق للنفاذ المباشر إلى المخدّم، ويجب أن يكون للمستخدم الـذي يريـد الوصـول إليـه حسابه الخاص على هذا المخـدّم ضمـن بيئـة UNIX. تسمح Telnet للمسـتخدمين بتحريـر الملفـات وتشغيل التطبيقات على المخدّم وتتطلب جزءاً صغيراً من موارد النظام، والعديد من تطبيقـات Telnet متوفر على شبكة الوب مجاناً.

Windows 95 Telnet

يأتي هذا التطبيق مع نظامي Windows 95 و Windows NT ، وهو مجاني ولكنه لا يملك الكثير من المزايا.

NCSA Telnet

هذا التطبيق مجاني أيضاً وهو تطبيق ماكينتوش شائع وكثير الاستخدام، غني بالمزايا ويستخدم جـزءاً بسيطاً من موارد النظام.

5- تطبيق الهاتف عبر الإنترنت وتطبيق المحادثة

تعتبر هذه التطبيقات جديدة نوعاً ما على شبكة الإنترنت، حيث يسمح تطبيق الهاتف عبر الإنترنت بإجراء مكالمة بين المستخدمين في الزمن الحقيقي وبدون تكاليف إضافية للمسافات البعيدة، أمّا تطبيق المحادثة فيقدم خدمة المحادثة بين المستخدمين عن طريق كتابة الرسائل وتبادلها آنياً.

وهناك العديد من البرمجيات التي تقوم بهاتين الخدمتين معاً، فمثلاً تعمل شركة Netscape بالتعاون مع شركة INSoft لإدخال هاتين الخدمتين إلى مستعرض Netscape، وقد تلحـق بـهما شـركتا IBM وMicrosoft.

3-3 الوصل مع الإنترنت

في الفصل السابق قمنا باستعراض كيفية النفاذ إلى الشبكة المحلية عن بعد، وفيما يلي سنتعرض لهذه التقنية ولكن من وجهة نظر الإنترانت، أي أننا سنركز الاهتمام في الناحية البرمجية وكيفية استخدام التجهيزات الفيزيائية لتحقيـق النفـاذ إلى الإنـترنت. يجـب في البدايـة تحديـد نـوع الخدمـات الـتي ستقدمها الإنترانت للمستخدمين قبل وصل الإنترانت مـع الإنـترنت، ليصبح بالإمكـان اختيـار نـوع الوصلة المناسبة. سنعرض فيما يلي تقنيات الوصل مع الإنترنت عموماً، وعادةً ما يكـون هـذا الوصـل بالاتفاق مع شركة معينة أو مؤسسة حكومية تكون موصولة مع الإنترنت، وتقدم هـذه الشـركة خدمـة الوصل مع الإنترنت لشركات أخرى أو للمستخدمين العـاديين، ونطلـق علـى هـذه الشـركات تسـمية مزودي خدمة الإنترنت ISP (Internet Service Provider).

3-3-1 طرق الوصل مع الإنترنت

آ – خدمة الاتصال التمثيلي عبر الهاتف (Dial-Up Analog Service).

يمكن للمستخدمين الذين يملكون موديمات موصولة إلى حواسيبهم الوصول إلى الإنترنت باستخدام هذه الخدمة، وأعلى سرعة يصل إليها الموديم في نقل المعلومات هي 28,800 Bps، ويمكن تحقيق سرعات أعلى بقليل على خطوط الهاتف التمثيلية، لكن السرعة السابقة تبقى السرعة القصوى التي يمكن تحقيقها.

يمكن الوصول إلى الإنترنت باستخدام هذه الخدمة بطريقتين: فإمّا أن نستخدم لكل حاسوب موديماً خاصاً به، أو أن نستخدم مخدّم اتصالات يدعم مجموعة من الموديمات يستطيع المستخدمون الوصول إليها عن طريق الشبكة المحلية. تُسمى الطريقة الأولى حسابات الأوامر (Shell Accounts)، والثانية حسابات SLIP و PPP.

1– حسابات الأوامر

يمكن النفاذ إلى حساب الأوامر عن طريق مجموعة من البرمجيات، مثل Windows Terminal، Procomm، PC Anywhere. عندما يتصل المستخدم مع مزود خدمة الإنترنت ISP وبعد إدخال هذا المستخدم يُوصل إلى حاسوب موصول مباشرة مع الإنترنت. هذا الحاسوب هو مخدّم يمتلك عنوان إنترنت وحيداً، ويسمح للمستخدمين المتصلين به باستخدام تطبيقات الإنترنت المثبتة عليه فيصبح بإمكانهم التجول على الإنترنت ؛ وهذه هي الطريقة الأولى لوصل المستخدمين عبر الموديمات.

السيئة الرئيسية في هذه الطريقة هي أنها لا تستخدم واجهات التخاطب البيانية، فالمستخدم الذي يستكشف شبكة الوب، من خلال حساب أوامر، سيستخدم برنامجاً مثل Lynx (مستعرض صفحات نصي) الذي يسمح له بقراءة صفحات الوب كنصوص بدون أي إمكانيات إظهار بيانية. وبالمقابل هناك فائدة من استخدام هذه الطريقة وهي أن المستخدم يستطيع استخدام برامج وتطبيقات المخدّم

التي تحتل مساحة واسعة من الذاكرة، حيث من الصعب والمكلف تخزينها على حاسوب المستخدم، لذلك فإن بعض المستخدمين يفضلون حسابات الأوامر كطريقة للنفاذ إلى الإنترنت.

2- *حسابات SLIP و PPP*

ساهم هذا النمط من الحسابات مساهمةً كبيرة في الانتشار الواسع لاستخدام الإنترنت، حيث يطلب المستخدم مزود خدمة الإنترنت (كما في الطريقة السابقة) الذي يقوم بوصله إلى الإنترنت، ولكن على العكس من طريقة حسابات الأوامر يتصل المستخدم مع مزوّد خدمة الإنترنت من خلال برمجيات SLIP أو PPP مثل Netscape dialer, Chameleon, Winsock، ويحصل بالتالي على عنوان إنترنت مخصص مباشرة لحاسوبه، ولهذا السبب يستطيع المستخدم استخدام التطبيقات والبرامج الموجودة على حاسوبه مثل تطبيقات البريد الإلكتروني وتطبيق Telnet وكذلك مستعرضات الوب البيانية.

يُخصص عنوان الإنترنت للمستخدمين المتصلين بمزود خدمة الإنترنت ديناميكياً، ولكن هذا لا يغير شيئاً من الناحية الوظيفية، رغم تغير العنوان الذي يدخل به المستخدم الإنترنت في كل مرة، حيث يقوم مزوّد خدمة الإنترنت بتخصيص العناوين عشوائياً من مجموعة من العناوين المعرّفة لديه مسبقاً.

ب ـ حسابات PPP و SLIP الهاتفية الرقمية

من الممكن الآن إجراء مكالمة رقمية بأسعار معقولة، وذلك بعد تطوير شبكات الهاتف لشبكات الخدمات المتكاملة الرقمية ISDN، حيث يمكن الحصول على سرعة نقل أعلى وبالتالي سرعة وصول أعلى إلى مواقع الإنترنت، وكما ذكرنا في الفصل السابق فإن أصغر سرعة تتعامل معها شبكات ISDN هي 56KBps ويمكن الوصول إلى سرعة 128KBps، مما يعني أن شبكات ISDN أكثر سرعةً من أسرع موديم.

تسمح شبكات ISDN للمستخدم بما يلي:

- البحث واسترجاع المعلومات بسرعة تفوق سرعة الوديم التمثيلي بمرتين أو أربع مرات.

- نقل الإشارة رقمياً إلى مزوّد خدمة الإنترنت عبر خطوط الهاتف.

في هذه الحالة يجب أن يستخدم مزوّد خدمة الإنترنت شبكة ISDN، حيث يجري الوصل معه من خلال جهاز TA الذي يقوم مقام الوديم، وكما في الحالة السابقة يحصل المستخدم على عنوان إنترنت لحاسوبه طوال فترة اتصاله.

ج - وصل الشبكة المحلية

توصل الشبكة المحلية باستخدام موجّه إلى مزود خدمة الإنترنت، مما يتطلب وجود برمجيات TCP/IP على الحواسيب التي ترغب بالوصول إلى الإنترنت، وهذه البرمجيات تختلف عن البرمجيات المستخدمة في حالة الوديم أو جهاز TA، حيث تسمح برمجيات TCP/IP للحاسوب بالتخاطب عبر الشبكة المحلية إلى الموجه ومن ثم إلى الإنترنت.

يمكن إجراء الوصل بطريقتين مختلفتين وفيما يلي تفصيل كل من هاتين الطريقتين (الشكل 3-5):

1- الوصل الدائم

في هذه الحالة تكون الوصلة بين الموجه والإنترنت مكرسة لهذا الاتصال دائماً، بمعنى أنه يوجد ممر أو دارة عبر شبكة الهاتف موصولة إلى مزود خدمة الإنترنت طوال 24 ساعة في اليوم. يُعتبر هذا النوع من الوصل مثالياً بالنسبة للمستخدمين الذين يملكون مخدّمات وب خاصة ويريدون أن تكون موصولة دائماً إلى الإنترنت، كما أن هذا النمط من الوصل مفضل في الشبكات المحلية ذات الحجم المتوسط أو الضخم من حيث عدد المستخدمين (أكثر من 25 مستخدماً)، وتكون سرعة الوصلة ضمن المجال 56KBps إلى 45KBps، وتختلف أنماط هذا النوع من الوصلات بحسب مزود خدمة الإنترنت وشركات الهاتف المحلية.

2- *الوصل المؤقت*

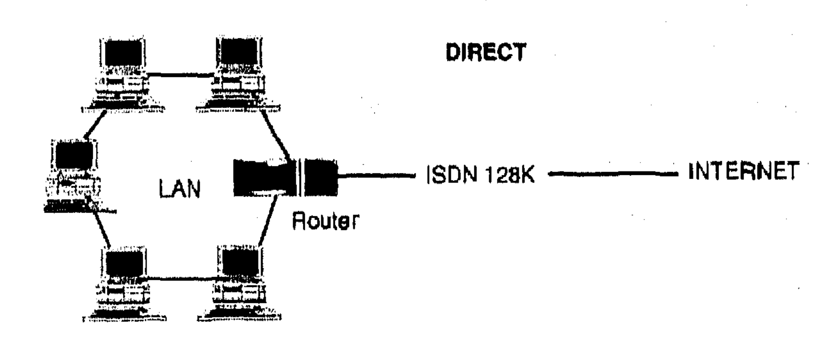
يعتمد هذا النوع على حجز خط للاتصال من قبل شركة الهاتف عند الطلب، ويحجز هذا الخط عندما يقوم أحد الحواسيب بطلب اتصال مع الإنترنت كتشغيل مستعرض وب، أو محاولة الوصول إلى موقع، أو إرسال بريد إلكتروني. يقوم الموجه عندها بعملية الوصل مع الإنترنت عند الحاجة ويلغي هذه الوصلة عند الانتهاء منها، ويعتبر هذا النمط من الوصل مثالياً بالنسبة للشبكات المحلية الصغيرة حيث تكون الاستخدامات قليلةً ومتباعدةً، ولكن إذا أردنا بناء موقع للوب على الشبكة المحلية فإن اختيار هذه الطريقة بالوصل ليس بالخيار الموفق، لأن الاتصال يجري من الشبكة المحلية إلى مزود خدمة الإنترنت باتجاه واحد فقط، ولا يمكن الاتصال بالاتجاه المعاكس.

LAN DIAL-UP

28.8Kbps Modem

LAN

INTERNET



الشكل (3-5): طرق وصل الشبكة المحلية

3-3-2 متطلبات الوصل مع الإنترنت

نحتاج إلى اختيار البنية المادية المتمثلة بالموجّـه، والبرمجيـات المتمثلـة ببرمجيـات TCP/IP لتحقيـق الوصل مع الإنترنت.

البنية المادية

الموجهات

لوصل الشبكة المحلية إلى مزود خدمة الإنترنت نحتاج إلى موجه سواء كان الوصل عبر شـبكة ISDN أو أي طريقة وصل مباشرة. وعلى الرغم من أنه من الممكن دوماً وصل الشبكة المحلية إلى مزود خدمـة الإنترنت باستخدام موديم إلاّ أن عرض حزمة النقل يظل محدوداً بـ 28KBps. يقـوم بعـض مـزودي خدمة الإنترنت بتأجير المعدات اللازمة لتحقيق عملية الوصل، وبالتالي يمكن توفـير جـزء مـن تكلفـة الإقلاع، وتلتغي مهمة اختيار الموجـه وتجـهيزه. وبمـا أن الموجـه يقـوم بتـأمين الوصـل بـين الشـبكة المحلية وشبكة واسعة النطاق، فإنه يجب أن يكون قادراً على توجيه البروتوكول TCP/IP.

يوجد عدد كبير من الموجهات المتوفرة حاليـاً مـن قبـل المصنعـين المعروفـين مثـل 3Com، CISCO، Ascend، Baymentworks ولكن الأشهر من بين الموجهات التي ظهرت خلال العقد الأخـير كـانت هي الموجـهات المصنعة من قبل شركة CISCO التي قامت ببناء سلسلة من الموجهات مثل:

- CISCO 2500: يؤمن الوصل بين شبكة محلية ومزود لخدمة الإنترنت ويحكم هذه الوصلـة البروتوكول TCP/IP.
- CISCO 3000 و CISCO 4000: يسـمح بإضافـة عـدة بطاقـات ربـط مـع مختلـف أنـواع الشبكات المحلية مثل TokenRing وإثرنت، وكذلك يصل بـين الشـبكات واسـعة النطـاق، فإذا أرادت شركة ما وصل أحد مكاتبها البعيدة إلى الإنترنت فهي بحاجة لموجه يتعامل مـع الشبكات واسعة النطاق مثل CISCO 4000.

- CISCO 7000: يُستخدم لوصل مزود خدمة إنترنت (أو مزود خدمة الإنترنت لمزودي خدمة الإنترنت) مع مزودي خدمة آخرين على الشبكة.

ولكن موجهات CISCO ليست الخيار الوحيد لوصل الشبكات المحلية مع الإنترنت، فهناك موجهات شركة 3Com التي تمتلك موجهات رخيصة الثمن مثل:

- 3Com 224 و 3Com 227 المكافئة لـ CISCO 2500.
- NetBuilder II المكافئ لـ CISICO 4000.

وتعتبر موجهات Ascend من الموجهات الشائعة الاستخدام لوصل الشبكات المحلية عن طريق وصلة مؤقتة سواء عبر شبكة ISDN أو موديم، من موجهات هذه الشركة نجد:

- Ascend Pipeline 130.
- Ascend Pipeline 50.

إذن هناك ثلاثة أنواع من الموجهات ولكن يمكن استخدام أي نظام قادر على التوجيه باستخدام بروتوكولات TCP/IP للوصول إلى الإنترنت.

تقوم كل الموجهات عموماً بنفس الوظائف، لكن توجد بعض النقاط المحددة التي يتطلبها مزودو خدمة الإنترنت أو دارة الشبكة الواسعة التي يجري الاتصال بها. فمثلاً إذا كانت لدينا شبكة محلية تحتوي على 75 مستخدماً ووصلة هاتف من النوع T-1 تصل الشبكة مع مزود خدمة الإنترنت فإن اختيار موجه CISCO 700 هو اختيار قاتل، ومن الممكن أن يكون CISCO 2500 اختياراً أكثر ملاءمة. أمّا إذا كان عدد المستخدمين لا يزيد عن 10 مستخدمين ونريد وصلهم في شبكة محلية ذات وصلة إنترنت مؤقتة فإن الحل الوحيد هو موجه Ascend pipeline 50.

البرمجيات

تحتاج الحواسيب التي تريد الدخول إلى الإنترنت إلى برمجيات TCP/IP، وتوجد عدة مجموعات من هذه البرمجيات، ولاختيار المجموعة المناسبة يمكن الاطلاع على مراجع عن هـذه التطبيقـات وأشـهر هذه المراجع هو O'Rielly Puplisher.

تحتوي معظم أنظمة تشغيل الشبكات المحلية مثل Netware أو Windows NT على دعم لبرمجيات TCP/IP أو يمكن أن تُضاف إليها ؛ ومن المجموعات التي يمكن الحصول عليها:

Netmanage's Chameleon أو برمجيات FTP مثل PC/TCP أو برمجيات IP مثل Wollen-gong. تعمل هذه البرمجيات في بيئة Windows وتؤمن عمل تطبيقات مثل البريد الإلكتروني أو Telnet على الشبكات المحلية، أما بالنسبة لحواسيب ماكينتوش فهناك برمجيات خاصة بها مثل MacTCP.

تسمح البرمجيات السابقة بالتعامل مع مختلف أنواع الشـبكات المحليـة: FDDI أو TokenRing أو إثرنت، ولكن يجب التـأكد دوماً مـن أن مجموعـة البرمجيـات الـتي نختارهـا تعمـل علـى الشـبكة المحلية، لذلك يجب التأكد من إعداد بطاقة ربـط الشـبكة NIC بمختلـف أنـواع الإطـارات المناسـبة لتسمح لبروتوكولات نظام تشغيل الشبكة المحليـة وبروتوكـولات TCP/IP بـالتواجد معـاً علـى نفس بطاقة ربط الشبكة.



الفصل الرابع

أمن الإنترانت

تحتاج أي شبكة نقل معلومات إلى نظام أمني يوفر حماية موارد الشبكة ويؤمن طريقة آمنة في تبادل المعطيات عبر هذه الشبكة. وإن فهم المخاطر التي قد يتعرض لها نظام تبادل المعلومات في الشبكة ونتائج هذه المخاطر يعتبر الخطوة الأولى في عملية بناء نظام أمني فعال للشبكة. فيجب أن يستند النظام الأمني على سياسة أمنية متعددة المستويات، بحيث يمكن تنظيم ومواجهة الأخطار العملية العالية التعقيد التي ترافق أي نظام نقل معلوماتي.

وتصنف الشبكات عموماً إلى قسمين من حيث أخطار الاختراق، حيث يمكن التمييز بين شبكات عامة، وشبكات خاصة. تتميز الشبكات الخاصة ـ ومنها شبكة الإنترانت ـ بتعرضها لأخطار اختراق يمكن أن تكون هدامةً، ومن ثم يجب أن تعتمد هذه الشبكات على نظام أمني يوفر حماية المعلومات من أخطار اختراق شديدة التعقيد. والمهمة الأساسية لنظام الحماية تكون في عزل نظام المعلومات في الشبكة عن مصادر الخطر المتعددة التي قد تؤدي إلى تسريب المعلومات السرية المخزنة، أو الإجرائيات والمعطيات الخاصة الخاضعة للنقل.

يمكن لنظام الحماية أن يخفق في حماية المعلومات نتيجة سوء إدارةٍ أو نتيجة حادثٍ عرضي مما قد يسبب ضرراً كبيراً للشركة من الناحية الأمنية، ولذلك يجب تزويد النظام الأمني بطرق عملية تستطيع كشف الأخطاء الأمنية، وتقدّم للشخص المسؤول عن ذلك تقريراً أمنياً من شأنه أن يساعد

على إيجاد الحل المناسب لمعالجة الإخفاق فور وقوعه، ويمكن تحقيق ما سبق بتزويد الشبكة بسياسة أمنية تنظم العمليات الأمنية الواجب القيام بها.

4-1 الأخطار المهددة لأمن الشبكة

يعتبر عزل شبكة الإنترانت عن مصادر الخطر المفتاحَ الأول في تحقيق أمن هذه الشبكة، ويكمن التحدي الأكبر هنا في النجاح بعزل شبكة الإنترانت عن كل المستخدمين الذين يحاولون الوصول على نحوٍ غير شرعي إلى موارد الشبكة، ويُسمى هؤلاء المستخدمون "المخترقين" (Hackers) على اختلاف غاياتهم.

4-1-1 أنواع الاختراقات

يمكن تصنيف المخترقين في نوعين أساسيين هما:

- المخترقون الخارجيون: هم المستخدمون من خارج شبكة الإنترانت والذين يجب منعهم من معرفة ما يدور داخل الشبكة.
- المخترقين الداخليون: وهم المستخدمون من داخل شبكة الإنترانت والذين قد تؤدي أخطاؤهم إلى وضع الشبكة في موقف حرج أمنياً دون أن يقصدوا ذلك.

ومن الجدير بالذكر أن عدد المخترقين الخارجين قد ازداد زيادةً كبيرة بعد تطوير تقنيات الوصل بين الشبكات وخصوصاً مع شبكة الإنترنت، حيث أن أغلب الاختراقات التي تحصل في شبكات الإنترانت تكون ناتجة عن وصلها مع شبكة الإنترنت العامة الاستخدام عالمياً، والتي تربط أعداداً لا تحصى من المستخدمين. وقد أدت عملية الوصل هذه إلى تشجيع هؤلاء المستخدمين الخارجين على اختراق شبكات الإنترانت وإلى تطوير تقنيات عالية المستوى لاختراق الأنظمة الأمنية المستخدمة

فيها، الأمر الذي يجبر شبكة الإنترانت، التي لا يمكنـها بـالطبع الاستغناء عـن الوصـل مـع شـبكة الإنترنت، على تطوير أنظمة أمنية شديدة التعقيد للحفاظ على وثوقية عالية ضد عمليات الاختراق.

ولسوء الحظ يعتبر المخترقون الداخليون أشد خطراً من غيرهم، حيث أنهم ينجحون أكثر مـن غـيرهم في عمليات الاختراق، وذلك باعتبارهم مستخدمين داخليين مما يجعلهم لا يخضعون لمعظم الإجراءات الأمنية المتشددة التي تطبق على المستخدمين الخارجين، وهم من جهة أخرى قد لا يقصدون الإساءة من خلال تصرفاتهم التي قد تشكّل خطراً لا يستهان به كما في إصدار معلومات حساسة عـن الشـركة دون قصد.

4-1-2 نقاط الضعف الأمنية

يستطيع أغلب المخترقين الوصول إلى موارد شبكة الإنترانت بسبب العديد من نقاط الضعف في النظـام الأمني المعتمد في الشبكة، وذلك بعد تحليل هذه النقاط وإيجاد الوسـائل المناسـبة لاستغلالها، لذلك يجب على النظام الأمني المتبع تحليل ودراسة هذه النقاط باستمرار وتطويـر التقنيـات الأمنيـة الـتي تدعم هذه النقاط وتسد ثغراتها. ويمكن أن نعرض نقاط الضعف الأمنية بعدة أشكال، وأكثر هذه النقاط شيوعاً هي نقاط الضعف العامة والأخطاء البشرية.

نقاط الضعف العامة (International Vulnerabilities)

غالباً ما نضطر للقبول ببعض نقاط الضعف في سبيل إنجاز مهام حيويـة وذات قيمـة عاليـة للشـركة. على سبيل المثال، قد تضطر الشركة لاستخدام بروتوكولات محددة أثناء بناء شبكة الإنترانت لأن هذه البروتوكولات معيارية (عالمية) كما أنها تقـدم الخدمـات المطلوبـة في المؤسسـة، ولا يمكـن أن تحصـل المؤسسة على مثل هذه الخدمات في حال استخدام أنواع أخرى من البروتوكولات، في حين قد تـؤدي هذه البروتوكولات إلى مشـاكل أمنيـة مـن جهـة أخـرى، وقـد تضطـر المؤسسـة إلى استخدام الوصـل اللاسلكي بين مكاتبها أو فروعها البعيـدة وهـذا الوصـل يـؤدي إلى مشـاكل اختراق لا يسـتهان بـها.

وعندما تضطر المؤسسة لاستخدام هذا النوع من البروتوكولات تقوم بتطوير نظام أمني شديد التعقيد لتدارك نقاط الضعف الموجودة في هذه البروتوكولات، مما يضطرها إلى إجراء دراسة وافية لمشاكل الاختراقات الأمنية التي قد تسببها هذه البروتوكولات.

الأخطاء البشرية

يحتاج أي نظام أمني إلى إدارة بشرية، وهذه الإدارة ترتكب بالطبع بعض الأخطاء التي لا يمكن تفاديها على نحوٍ مطلق أثناء عملية إعداد وإدارة أنظمة أمن الشبكة، وتُستغل هذه الأخطاء من قبل المخترقين.

الجزء الأكبر من الأخطاء البشرية ينتج عن الطبيعة الديناميكية للشبكة، إذ تُدخل دوماً عناصر جديدة إلى الشبكة لتحل محل العناصر القديمة، إضافةً إلى اعتبارات النمو السريع وإعادة التنظيم وتقليص عدد العاملين ودمج النشاطات مع أنشطة مؤسسات أخرى، وغيرها من التغيرات التي يمكن حدوثها، وكل هذه التغيرات مرشحة لخلق هذا النوع من المشاكل الأمنية وخصوصاً في ظلّ النقص في الأشخاص من ذوي الخبرة والمدربين تدريباً مناسباً لمواجهة مهام الإدارة الأمنية. لذلك من الضروري جداً الاعتماد على أشخاص محترفين للقيام بهذه الواجبات، وللحصول على نتائج مقبولة بالرغم من وجود بعض الأخطاء التي لا يمكن تفاديها والتي تؤدي إلى اختراق متوقع من قبل مخترقين يترقبون حدوث هذا النوع من الأخطاء بعد اعتماد الشكل النهائي للنظام الأمني المتبع.

4-1-3 الوصل مع الإنترنت

يجري وصل شبكة الإنترانت مع الإنترنت في العديد من المؤسسات وذلك بهدف الحصول على خدمات الإنترنت التي لا يمكن الاستغناء عنها في المؤسسة. لأن شبكة الإنترنت تقدم للمؤسسة خدمات من شأنها زيادة إنتاجية العاملين وتأمين الاتصال المباشر مع الزبائن والمولين والشركاء، وتسهيل استخدام التكنولوجيا العالمية المتطورة. وتتعرض الإنترانت في المؤسسة إلى أكثر المشاكل

الأمنية خطورة نتيجة وصلها مع الإنترنت مقابل الخدمات التي تقدمها الإنترنت، فهذا الوصل من شأنه ربط محطات العمل المحلية والمحدودة على شبكة الإنترانت مع شبكة عالمية لا يمكن حصر عدد محطات العمل فيها، وتكون هذه الأخيرة قادرة على الوصول إلى موارد شبكة الإنترانت عن طريق الإنترنت. كما يضمن هذا الوصل بالطبع قناة اتصال ذات حزمة تمرير ضخمة إلى قلب الشبكة الداخلية.

ويجري الاعتناء بهذه القناة عادةً بتشكيل ما يدعى بالجدار الناري (Firewall)، الذي يقوم ببناء حاجز بين الشبكتين، ولكن إذا قام أحد المتطفلين باستغلال نقاط ضعف الجدار الناري فإنه قد ينجح باختراق الشبكة.

يشعر معظم مدراء شبكات الإنترانت بأن شبكاتهم آمنة نسبياً وأنه من غير المتوقع أن يقوم أحد المتطفلين باختراق الشبكة، خاصةً إذا كان النظام الأمني قد طُوِّر تطويراً ملائماً لمنع حدوث عمليات الاختراق، ولكن هذا التفكير خاطئ أمنياً، إذ أن نسبة كبيرة من السياسات الأمنية المتبعة تتعرض للاختراق بسبب عدم اعتمادها على تقنيات كشف وتسجيل الحوادث الأمنية عند حدوثها، إضافةً إلى دراسة هذه الحوادث ومحاولة معالجتها فور حدوثها، فمن المحتمل أن يكون المخترق ناشطاً وغير مكشوف بالنسبة للشبكة، وعندها يكون مدير الشبكة غير قادر على كشف هذا النشاط لعدم وجود أي تقنية فعالة لذلك.

وللسبب السابق ذاته فإن المعايير الأمنية المتبعة حالياً في كل الشبكات الافتراضية تفرض استخدام نظام تنبيه للإدارة عند حدوث أي نشاط ملحوظ لاختراق الشبكة، مما يمكّن مدير الشبكة من التفاعل مع نشاط الاختراق في اللحظة التي ينجح فيها بمعرفة مدى فعالية هذا الاختراق وهي اللحظة التي يكون المتطفل فيها غير حذر، أو يصبح نشاطه تدميرياً.

وهكذا، إذا جرت السيطرة على الأخطار العملية المهددة لأمن الشبكة فإن القدرة على الكشف والاستجابة فور وقوع الخطر أمر بالغ الأهمية، وفي حال عدم تحقيق ذلك سيصبح من المستحيل حصر الاختراقات التي قد تتعرض لها الشبكة. ويجري بناء أنظمة الكشف والاستجابة للخطر بواسطة

برمجيات متطورة جداً تراقب حركة نقل المعطيات عبر الشبكة، وتقوم بفحص مستمر ودائم لأي نشاط غير مسموح به عبر الشبكة، وعند كشف أي نوع من هذه النشاطات تقوم هذه البرمجيات آلياً بالاستجابة ضد هذا النشاط باتباع إجرائيات مصممة سلفاً، فقد تقوم مثلاً بتسجيل هذه النشاطات وإعداد تقارير عنها تُرفع إلى مدير الشبكة، أو تقوم فوراً بالنفاذ إلى مكان الحدث لمعالجته آنياً، أو تقوم بإنهاء الاتصال الذي حدث فيه الاختراق.

4-2 السياسة الأمنية المتبعة

يقصد بالسياسة الأمنية (Security Policy) الإجراءات الواجب اتباعها للحفاظ على أمن شبكة الإنترانت، وتتألف هذه الإجراءات من حلول تقنية وقرارات أمنية تتآلف فيما بينها لجعل موارد الشبكة آمنة وصعبة المنال بالنسبة للمخترقين. وعند تصميم السياسة الأمنية تؤخذ نقاط ضعف الأمن في الشبكة بعين الاعتبار، وتوضع قوانين ناظمة للتعبير عن كل ما يجب فعله بخصوص الشبكة وما لا يجب فعله.

الجزء الأهم في بناء السياسة الأمنية هو كتابة وثيقة تُوصِّف النقاط الأكثر حساسية والأكثر حاجة للحماية في الشبكة، وعند اعتماد الصيغة النهائية للسياسة الأمنية الواجب اتباعها يجري إصدار هذه السياسة في وثيقة مكتوبة تعبّر بصراحةٍ ووضوحٍ عن كل ما هو مسموح وممنوع عبر الشبكة. تسمح هذه الوثيقة بتقييم فاعلية كل الإجراءات الأمنية التي تتبعها الشبكة للحفاظ على أمن مواردها، كما أنها تشرح للمستخدمين على الشبكة و لإدارة الشبكة القواعد والضوابط الواجب اتباعها عند استخدام الشبكة.

كتابة الوثيقة الأمنية عملية معقدة نوعاً ما، فهي تتطلب فهماً شاملاً لكل بيئات العمل في الشبكة ولكل مواردها ومتطلباتها، إضافةً إلى تحديد كل الاتصالات الممكن القيام بها عبر الشبكة سواء أكانت اتصالات داخلية أم خارجية مع شبكة الإنترنت أو شبكات إنترانت أخرى. وتوجد بالطبع خطوط عريضة يمكن شرحها عند كتابة الوثيقة الأمنية الخاصة بأي شبكة، فهذه الوثيقة تتطلب الإحاطة

بالأفكار العامة إحاطة كافيةً للحصول على خاصية المرونة من جهة، إضافةً إلى ضرورة كونها دقيقة جداً وذات مغزى مفيد من جهة أخرى.

4-2-1 كتابة الوثيقة الأمنية

تتألف الوثيقة الأمنية من جزأين رئيسيين، يضم الجزء الأول فرع الأمن، ويُوصِّف هذا الفرع كل ما هو بحاجة إلى الحماية عبر الشبكة توصيفاً دقيقاً جداً، ويحدّد الطرق الواجب اتباعها والإجراءات الأمنية الخاصة لتوفير الحماية المطلوبة لكل مورد تجب حمايته على حدة. في حين يتألف الجزء الثاني من القواعد الناظمة لعملية النفاذ إلى الشبكة حيث يجري تحديد السماحيات المكنة للنفاذ إلى الشبكة من قبل المستخدمين، كما يجري تحديد كل ما يمكن أن يفعله المستخدمون عند نفاذهم إلى موارد الشبكة.

الجزء الأول: تحديد الموارد

توصّف الوثيقة كل موارد الشبكة المطلوبة حمايتها في الجزء الأول منها وهذا الجزء هو الأكثر صعوبة، إذ أن تحديد ما يمكن استخدامه في الشبكة ليس بالأمر السهل حيث أن أغلب المستخدمين ليس لديهم إحاطة كاملة بالموارد التي يستخدمونها، وبدرجة أهمية هذه الموارد بالنسبة لأمن شبكة الإنترانت. ولهذا السبب يفضل تقسيم المستخدمين في مجموعات جزئية بالنسبة لإدارة الشبكة، وتحديد الملفات والبرامج التي تستخدمها كل مجموعة على حدة، وتنظيم قائمة تحتوي على مجموعات المستخدمين وعلى الموارد التي تستخدمها كل مجموعة.

ويفضل عند كتابة الوثيقة عدم استخدام أسماء الملفات مثلاً كمورد لهذه المجموعات، حيث أن هذه الأسماء قد تتغير على نحو متواتر، مما يفقد الوثيقة الأمنية مرونتها المطلوبة ويؤدي إلى ضرورة تغييرها. و يُتّبع عادةً نظام تقسيم للملفات بالنظر إليها كمورد لمجموعات المستخدمين مما يسمح للوثيقة الأمنية بتوصيف مرن لهذه الملفات. فعلى سبيل المثال يجري تقسيم الملفات في المؤسسات

تقسيماً يتفق مع أقسام هذه المؤسسات، كالملفات الخاصة بالقسم المالي واعتبار هذه الملفات كمورد بحاجة إلى حماية عالية مقارنة بملفات قسم الإنتاج مثلاً. وهذا ما يعطي للوثيقة الأمنية مرونة كبيرة تسمح بحدوث بعض التغييرات دون الحاجة إلى إعادة كتابة الوثيقة، وتبقى هذه الوثيقة بالمقابل دقيقة في مسألة تحديد الموارد الحساسة أمنياً.

الجزء الثاني: سماحيات النفاذ إلى الموارد

يُحدِّد الجزء الثاني من الوثيقة بدقة الجهات القادرة وتلك غير المسموح لها بالوصول إلى الموارد المذكورة في الجزء الأول، ويبنى هذا الجزء عادةً على شكل طبقات متراكبة، بحيث تتوافق الطبقة الأعلى مع الأجهزة الأكثر حساسية في الشبكة الداخلية، خاصة تلك الأجهزة المسؤولة عن تنظيم عمل المستخدمين والتي تقدم دعماً جيداً للسياسة الأمنية ويجب أن تكون مخفية عن مجموعات المستخدمين.

أما الطبقة الثانية من المعلومات فهي التي تكون متاحة للتعديل من قبل مجموعات إدارية ومن الممكن أن تكون قابلة للقراءة من قبل بعض مجموعات المستخدمين، وبالطبع يجب تحديد المجموعات المسموح لها بالدخول إلى هذه الطبقة، وتحديد احتياجات كل من هذه المجموعات وتلبيتها وفقاً لقواعد أمنية مدروسة.

تكون الطبقة الثالثة مقروءة عادةً من قبل جميع مجموعات المستخدمين، ولكن سماحية الكتابة فيها محصورة في بعض المجموعات فقط وليست متاحة لجميع المستخدمين.

أما الطبقة الأخيرة من المعلومات فتكون قابلة للقراءة والكتابة من قبل جميع مجموعات المستخدمين.

تقع شبكة الإنترانت عادة في إحدى الطبقات السابقة وذلك حسب المؤسسة، فقد تسمح بعض المؤسسات لمجموعة محددة فقط من العاملين فيها بتحديث معلومات المواقع، الأمر الذي قد يقلل من إرسال المعلومات غير الدقيقة خارج الشركة، بينما تقوم مؤسسات أخرى بالسماح لأغلب العاملين

فيها بالتعامل مع معلومات المواقع وبذلك تحملهم مسؤولية أكبر تجاه المؤسسة، ولا سيما عندما يتعلق الأمر بالمعلومات التي قد تكون حساسة عند إصدارها إلى العالم الخارجي.

ومن الجدير بالذكر، أن الوثيقة الأمنية المعبرة عن السياسة الأمنية لشبكة الإنترانت لا تتعامل تعاملاً محدداً وواضحاً مع عمليات النفاذ الخارجية إلى شبكة الإنترانت من قبل مستخدمي الإنترنت، حيث أنها تفترض أن المستخدمين على الإنترنت يقعون ضمن الطبقة الثالثة في طبقات سماحيات الوصول المذكورة أعلاه، أي أنه بإمكان هؤلاء المستخدمين قراءة أي وثيقة مسموح بها للمستخدمين الداخليين. ولكن لحسن الحظ أن هذه السماحية غير موجودة عملياً بسبب وجود تقنيات تمنع هذا النفاذ الخارجي، ولكن هذا الافتراض يحثّ على البدء بالتجهُّز له.

بعد كتابة الوثيقة الأمنية تجب مراجعة هذه الوثيقة من قبل جهة قانونية لإعطائها صفة الإلزام بما يتلاءم مع احتياجات الإدارة العليا، ولإضافة ما تحتاجه هذه الوثيقة كي تنفّذ قسراً من قبل الإدارة العليا على مجموعات المستخدمين، وإذا لم توافق الإدارة العليا للشبكة على السياسة الأمنية فإن الوثيقة لا معنى لها، وتجب إعادة صياغتها وتدارك نقاط ضعفها.

وهكذا، فإن كتابة الوثيقة الأمنية تهدف إلى تحديد الخطوط العامة في توصيف السياسة الأمنية للشبكة، وينصح قبل البدء في كتابة أي وثيقة أمنية بالاطلاع على عينات من هذه الوثائق المكتوبة مسبقاً والمتاحة من قبل شركات عالية لاستخدامها كأمثلة تساعد على كتابة الوثائق الأمنية الخاصة بالشبكة المطلوبة. ويمكن استقدام وثائق أمنية من أحد المواقع التالية:

http://delphi.colorado.edu/~pubs/draft9.html

gopher://gopher.eff.org/11/CAF/policies

http://www.crmwc.com/aup.htm

http://chico.rice.edu/armadillo/acceptable.html

http://all.net/books/policy/top.html

قد لا يُوصِّف أيٌّ من الوثائق السابقة الاحتياجاتِ الحقيقيةَ المطلوبة لإنترانت محددة نسعى إلى تزويدها بسياسة أمنية خاصة، ولكنها قد تساعد في شرح الخطوط العريضة في عملية كتابة الوثيقة

الأمنية (ما الذي يجب أن تحتويه هذه الوثيقة)، ومن ثـم تُطـوِّر هـذه الخطـوط العريضـة بتـلاؤم مـع احتياجات الشبكة الحقيقية.

4-2-2 نقاط ضعف الوثيقة الأمنية

عند كتابة الوثيقة الأمنية يجب توخي الحذر الشديد والاهتمام بدقة التعابير المستخدمة فيـها، وعنـد حدوث حالات نزاع وتنافس بين أطراف معينة تجب مراجعة هـذه الوثيقـة مـن قبـل طـرف قـانوني مختص بقوانين المعلوماتية، ومن ثم تصديق هذه الوثيقة من قبل الجهات المختصة.

ومن الأشياء التي ينبغي تذكرها جيداً أنه يجب على الوثيقة الأمنيـة تحديـد كـل مـا هـو مسـموح أو ممنوع في الشبكة دون إغفال أي شيء، لتجنب الوقوع في مشاكل أمنية غير قابلة للمعالجة بسـبب أن الوثيقة الأمنية لا تنص على هذه المشاكل. فعلى سبيل المثال، إذا ذكـرت إحـدى الوثـائق الأمنيـة في أحد بنودها: عدم السماح لأي شخص بالنفاذ إلى القسم المالي (باستثناء العاملين فيه طبعاً)، وقام أحد المدراء بالنفاذ إلى هذا القسم، وهو يملك الصلاحية الإدارية لذلك، فإن هذه الوثيقة تعتـبر ضعيفـة لأن هناك طريقة للدخول إلى هذا القسم من قبل شخص ما، حتى ولو كانت هذه الطريقة غير شـرعية مـن وجهـة نظر الوثيقة الأمنية. وللتخلص من هذه الهفوة، كان على الوثيقة أن تنص حرفياً على أن يُمنع أي شخص من الدخول إلى القسم المالي إلا بإذن مـن مديـر الشـركة، وفي هـذه الحالـة يجـري السـماح لبعض الأشخاص دون سواهم بالدخول إلى هذا القسم دون أي مشاكل أمنية.

كما يجب أخذ مشاعر العاملين في المؤسسة بعين الاعتبار عند كتابـة الوثيقـة الأمنيـة، وخاصـة تلـك الشركات التي تحتاج منظومـة العمـل فيـها إلى عـاملين ذوي روح معنويـة عاليـة. فقـد يشـعر بعـض العاملين بالاستياء تجاه بعض التعابير اللاذعة المستخدمة في الوثيقة لردعهم عن القيام ببعض الأعمال عبر الشبكة، ومن ثم ينعكس هذا الاستياء على أدائهم المهني في الشركة بسبب نقمتهم تجاهها، وهذا بالطبع لا يعني السماح لهم بفعل ما يريدونه على شبكة الإنترنت مثلاً، بل إعطاءَهم بعض الثقة التي من شأنها أن تدعم الميثاق الأمني المتبع في شبكة المؤسسة.

4-2-3 نماذج السياسة الأمنية المتبعة

يختلف النموذج الذي تتبعه السياسة الأمنية باختلاف معايير الأمن في الشبكة الواجبة حمايتها. فتحتاج بعض المؤسسات إلى نظام أمني مشدّد جداً بسبب حساسية عملها ومنافستها التجارية. وهناك مؤسسات علمية (كالجامعات والمعاهد) قد لا تحتاج بالضرورة إلى نظام حماية شديد التعقيد، بسبب أهمية عملية تبادل المعلومات العلمية التي يجب أن تكون مفتوحة، ومن ثم فإن الموارد الواجبة حمايتها في الإنترانت الخاصة بهذه المؤسسات ليست كثيرة، كما أنه من غير الضروري حمايتها من كل المستخدمين الخارجيين والداخليين.

يوجد عموماً نموذجان رئيسيان لتوصيف السياسة الأمنية لشبكة الإنترانت وفق خطوط عامة، ويختلف هذان النموذجان من حيث طبيعة الحماية الأمنية المطلوبة، ويعتمد كل منهما على سياسة منع وسماح خاصة به، وهما:

- كل ما هو غير مسموح ممنوع: يعتمد هذا النموذج بدايةً على عدم السماح لأي شخص بالنفاذ إلى المورد، ومن ثم السماح لمجموعة محددة من الأشخاص بالنفاذ إلى هذا المورد، وهكذا فإنه وفقاً لهذا النموذج فإن المنع عام والسماح خاص.
- كل ما هو غير ممنوع مسموح: يعتمد هذا النموذج بدايةً على السماح لأي شخص بالنفاذ إلى المورد، ومن ثم تحديد مجموعة محددة من الأشخاص الواجب منعهم من النفاذ إلى هذا المورد، وهكذا فإنه وفقاً لهذا النموذج فإن السماح عام والمنع خاص.

من الواضح أن النموذج الأول أكثر تشدداً من الناحية الأمنية، حيث أن عملية النفاذ للمورد تكون محدودة ببعض المستخدمين، وهو النموذج المستخدم في الأنظمة الأمنية المتشددة. في حين يُعتبر النموذج الثاني متساهلاً إلى حد كبير بالمقارنة مع النموذج الأول، ويُستخدم هذا النموذج عادةً في الأنظمة التي تحتاج إلى تبادل معلوماتي مفتوح، إلا بالنسبة لبعض الجهات المحدّدة.

4-2-4 تثقيف المستخدمين

إن تثقيف المستخدمين هو من الخطوات الأكثر أهمية من الناحية الأمنية، فعند السماح لهم بالنفاذ إلى شبكة الإنترانت يجب تدريبهم علـى كيفيـة اسـتخدام هـذه الشـبكة، لأن الاسـتثمار الخـاطئ لـموارد الشبكة من قبل بعض المستخدمين الداخليين قد يؤدي إلى مخاطر أمنية لا يستهان بها.

ويقوم المستخدم عادةً باتباع دورات تأهيلية قبل السماح له باستخدام الشبكة، وهذه الـدورات تخولـه للنفاذ إلى الشبكة بعد تعليمه العديد من التقنيات اللازمة لذلك، وغالباً ما تغطي هذه الدورات العديـد من النقاط، ومن أهمها:

- *NEtiquette*: ويُقصد بهذا التعبير "آداب الشبكات"، حيث يعطى المستخدم معلومـات عـن كيفية القيام بأمور بسيطة، مثل الطريقة الصحيحة للاشتراك في قائمة البريد، وعـدم إرسـال رسائل بريد إلكترونية شخصية إلى قوائم البريد، وعدم إرسال إعلانات واضحة لجهات غـير مسموح لها بالاطلاع عليها، وغيرها مـن الآداب العامـة والسـلوكيات الواجـب اتباعـها عنـد استخدام الشبكة.
- *كيفية عمل البرمجيات في الشبكة*: وتتضمن هذه المرحلة تعريـف المسـتخدمين بكيفيـة عمـل بعض البرمجيات الهامة التي قد تصادفهم أثناء العمـل في الشـبكة، ويجـب أن تغطـي هـذه المرحلة كل الأدوات الممكن استخدامها في الإنترنت مـن قبـل الإنـترانت كمسـتعرض الـوب، وخدمة نقل اللفات، وتطبيق Telnet، والبريد الإلكتروني.
- *الأمن*: يجري في هذه المرحلة إرشاد المستخدمين وإطلاعهم على التعليمات الأمنية الأساسـية والتأكيد على ضرورة اتباع هذه التعليمات، وبيان المخاطر المترتبة على عدم اتباعـها، ومنـها حماية البريد الإلكتروني، وكيفية استخدام ووضع كلمات سر جيدة، وضرورة عدم إرسال أي وثائق حساسة عن الشركة إلى قوائم البريد، وغيرها.

- *المسؤولية*: تُشرح للمستخدمين في هذه المرحلة كيفية اتباع الطرق الصحيحة في الاتصال، وتستطيع إدارة الشبكة تجنب الكثير من المشاكل الأمنية إذا قامت بإعداد دورات تأهيل جيدة لكل المستخدمين، لتدريبهم على التعامل مع شبكة الإنترانت بحسّ عالٍ بالمسؤولية.

  ولرؤية الانعكاس السلبي على المؤسسة نتيجةً لما قد يرسله العاملون، يكفي بأن تقوم إدارة الشبكة بعملية بحث عن اسم الشركة في واحد من محركات البحث الكبيرة واستعراض نتائج هذا البحث أمام العاملين، وسوف تكون النتيجة مفاجئة للجميع.

وهذه الدورات التدريبية ستقلل من الأخطاء التي قد يرتكبها المستخدم عرضاً والتي قد تؤثر على أمن الشبكة، كما أنها سوف تقلل من إضاعة الوقت في الإنترانت نتيجة تكريسها لخدمة الأهداف الشخصية.

وتقوم أغلب الشركات بإعداد ملفات تحتوي على عمليات إحصائية تسجل أرقاماً حول مدى استخدام المستخدمين للشبكة، وتحتوي هذه الملفات على الأقسام التالية:

- *الحجم*: ويدل هذا القسم على عدد الثمانيات المستقدمة من شبكة الإنترنت خلال كل اتصال، وتساعد هذه الإحصائية على تنظيم فواتير الموظفين أو الأقسام، أو قد تساعد في حساب عرض حزمة الإرسال المستخدمة.
- *الاسم*: ويدل هذا القسم على اسم الوثيقة (مثل index.html أو button.gif) وقد يعطي هذا الاسم دلالات عن محتوى الوثيقة.
- *الزمن والتاريخ*: يدل هذا القسم على زمن وتاريخ عملية الاستقدام، لأن بعض الوثائق الأمنية تسمح بالاستخدامات الشخصية للشبكة خارج أوقات العمل فقط.
- *اسم الموقع*: ويحدد هذا القسم اسم الموقع البعيد الذي جرى الاتصال به، وهذا يساعد في معرفة ما إذا كان لهذا الموقع علاقة بالعمل أو لا.
- *البوابة الهدف*: وقد تكون بوابة FTP أو HTTP أو غيرها، وتحدد هذه البوابة عادة اسم البروتوكول الذي قام بعملية الاستقدام.

ومن الجدير بالذكر أنه قد لا تتمكن إدارة الشبكة من تحديد اسم الملف أو اسم البوابة الهدف، فمن الممكن أن تسمى الملفات بأسماء أخرى ليس لها أي امتداد ولا تتعلق بمحتوى الملف في حال استخدام الوكيل (Proxy)، وهذه المخدّمات قد تعمل على بوابات غير قياسية.

يضمن الكثير من المواقع وضع فواتير للاستخدام مما يجعل الأقسام مسؤولة عن استثمار الموارد وعن استخدام حزمة التمرير المتاحة في الشبكة، كما تساعد هذه الفواتير على الأقل في معرفة الأقسام الأكثر مسؤولية عن استخدام حزمة التمرير المتاحة. وتحتوي مواقع أخرى على لوائح تضم أسماء المستخدمين العشرة الأوائل (Top Ten Users) الأكثر استخداماً للشبكة، أو أسماء المواقع العشرة الأوائل (Top Ten Sites) ومن الطبيعي في هذه الحالة أن لا يرغب العاملون بأن تكون أسماؤهم على قائمة العشرة الأوائل على الموقع (www.wastetime.com) والتي ترفع إلى إدارة الشبكة دورياً، مما يحد من استخداماتهم الشخصية.

يُعتبر استخدام نظام محاسبة العاملين للحد من استخدام الإنترنت استخداماً سيئاً أفضل بكثير من اللجوء إلى تقنيات أخرى لمنع بعض عمليات النفاذ، مثل ترشيح عمليات النفاذ وفق قائمة منع محددة مسبقاً تضم عناوين مواقع شهيرة أو عناوين المواقع التي تضم كلمة معينة قد تحدد غالباً محتوى الموقع، ويسمح هذا النظام بعلاقات جيدة بين الإدارة والعاملين، وذلك عندما يرى العاملون أن الشركة تمنحهم الثقة معتبرةً أنهم لا يضيعون الوقت، وإنما تحاول إدارة الشركة المحافظة فقط على مسارات محددة ضمن عرض حزمة النقل المتاح في الشبكة والتي يجب أن تستخدم استخداماً مفيداً لمصلحة الشركة.

4-3 الأمن من خلال التمويه

يعتبر التمويه من أسهل الطرق المتبعة في النظم الأمنية، وفيه تجري حماية شبكة الإنترانت من النفاذ غير المسموح به من قبل المستخدمين العاديين بجعلها غير مرئية لهم (سنشرح تقنيات هذا التمويه لاحقاً). ولا يعتبر التمويه حماية أمنية حقيقية للإنترانت حيث أنها لن تصبح مخفية عن كل من

يحاول اختراق موقعها، ولكن هذه التقنية قد تبعد بعض المخترقين عنها فقط، وهذه الطريقة في الحماية لا تتعدى كونها عملية تعمية بسيطة، والتعمية بالتعريف هي جعل الموقع غير مرئي، ولكن إذا تم العثور على هذا الموقع من قبل أحد المتطفلين من قبيل الصدفة فمن المحتمل أن تكون النتائج غير محمودة.

ويعتبر التمويه أمراً جيداً ومطلوباً دائماً، فهو طريقة مناسبة تجعل المخترق يضيّع بعض الوقت للعثور على موقع الشبكة، مما يسمح للموقع بإطلاق إنذار أمني للشخص المسؤول حالَ كشفِ نشاط المخترق. وغالباً ما يتطلب الدفاع الجيد عن أمن الشبكة تكاتف العديد من الإجراءات الأمنية مثل أمن المخدّمات والجدار الناري، إضافةً إلى التمويه، مما يؤدي إلى كشف الاختراق أثناء محاولة المخترق البحثَ عن نقاط الضعف قبل قيامه باستغلالها للنفاذ إلى الشبكة.

تستخدم عدة طرق لتحقيق تقنية التمويه، وتعتبر الطرق الثلاث التالية من أهم الطرق المستخدمة في التمويه وهي:

4-3-1 استخدام بوابات غير قياسية

يمكن إخفاء موقع الإنترانت عن شبكة الإنترنت باستخدام بوابات غير قياسية مما يؤدي إلى حجب البوابات الحقيقة عن المستخدمين الفضوليين أو المخترقين القادمين من خارج الإنترانت. وتستخدم معظم مخدّمات الوب تشكيلاً بسيطاً يسمح لإدارة الإنترانت بتغيير رقم البوابة، فالبوابة القياسية المستخدمة عادة هي البوابة 80 وبتغيير رقم البوابة من 80 إلى أي رقم آخر سوف يصعُب كثيراً العثور عليها، وفيما يلي بعض الأمثلة عن كيفية تغيير رقم البوابة على بعض مخدّمات الوب الشهيرة:

تغيير رقم البوابة في مخدّم Apache

يمكن إنجاز هذه العملية بسهولة وبطريقتين مختلفتين وذلك بحسب طريقة تشغيل Apache، فإذا كان Apache يعمل من خلال Inted (في بيئة UNIX) فعندها يجب تحرير الملف /etc/inetd.conf وتغيير الرقم 80 إلى أي رقم آخر ليصبح الرقمَ الجديد للبوابة، ومن ثم نعيد تشغيل Inetd عن طريق

إرسال إشارة HUP إليه (بواسطة التعليمة "kill –HUP pid" حيث pid هو رقم محدّد الإجراء Inetd). أما إذا جرى تشغيل Apache عن طريق برنامج دفعي مثل rc.local فعندها يجب تحرير الملف httpd.conf الموجود في المجلد http/conf، حيث يوجد سطر في هذا الملف يحوي موجه البوابة وهو يستخدم رقم البوابة 80 افتراضياً، وبتغيير بسيط لهذا الرقم يمكن الحصول على بوابة برقم مختلف وذلك بعد إعادة تشغيل Httpd من جديد.

تغيير رقم البوابة في مخدّم الوب NetWare

يمكن إجراء التغيير المطلوب باستخدام برنامج إدارة مخدّم الوب، وبأخذ الخيار "مخدّم" من القائمة "ملف"، ثم مخدّم، ثم اختيار السواقة التي يتعامل معها مخدّم الوب، وعندها نغيّر رقم بوابة TCP إلى رقم آخر غير 80، ونضغط زر OK، ومن ثم نحفظ التغييرات ونعيد التشغيل، فيكون التغيير المطلوب قد أنجز.

تغيير رقم البوابة في مخدّم Netscape

يمكن إجراء هذا التغيير باستخدام برنامج مدير المخدّم، حيث نبدأ بتشغيل start-admin ومن ثم عبر المستعرض نختار صفحة مدير المخدم، ومن ثم نذهب للعنوان http://intranet.server.name:aport/ وبالطبع فإن القسم الأول intranet.server.name هو اسم مخدّم الإنترانت، أمّا aport فهي البوابة التي نريد التحكم بها، وبتغيير رقم البوابة وإعادة التشغيل، يصبح للبوابة رقمٌ جديدٌ غير الرقم المعياري 80.

4–3–2 استخدام أسماء صعبة التخمين

ترغب معظم الشركات بأن يستطيع الجميع العثور على مواقع الوب الخاصة بها بسرعة وسهولة، ولذلك فإن هذه الشركات تستخدم عادة أسماء مثل www.compny.com مما يجعل الاسم سهل التذكر، ومن غير الضروري أن تقوم الشركة بتسمية مخدّم الوب باسم الشركة إذ من الممكن تسميته

باسم آخر غامض قليلاً مثل: udu33rf.company.com، الأمر الـذي لا يوفـر فرصـة جيـدة لتخمـين معنى هذا الاسم والعثور على الموقع بسهولة.

4-3-3 إخفاء اسم المخدّم

تعتبر الطريقة السابقة في التمويه غير ناجحة عملياً إذا كـان الاسـم مدرجـاً في مخـدّم الأسمـاء DNS (Domain Name Service)، أو في حال ظهور اسم مخدّم الـوب في عمليـات النفـاذ العامـة للشـبكة. ولذلك تتبع عادةً طريقة أفضل منها وهي إخفاء اسم المخدم مما يجعل عملية إيجاده من قبل المتطفلين عملية صعبة التحقيق، ويجري إخفاء اسم المخدم عن طريق إعداد المخدم وفق خطوات محددة.

ملاحظة

يسمح النظام DNS للمواقع في شبكة الإنترنت بمعرفة الجهة التي تتخاطب معها، وهـو مـزود بنظـام توزيع للأسماء يسمح لكل موقع بالحصول على لائحة خاصة به بأسمـاء الحواسـيب المضيفـة المقابلـة لعنوان IP الخاص بكل موقع.

الإخفاء باستخدام مخدّمات أسماء منفصلة

تستخدم بعض المواقع أسماء مخدّمات منفصلة داخلية وخارجية، مما يسمح لمحطات العمل الداخلية في الشبكة بالاتصال مع مخدّم الإنترانت بواسطة الاسم الداخلي دون تسريب أي معلومات إضافية إلى الإنترنت.

وتجري هذه العملية وفق ما يلي:

عندما يرغب أحد المستخدمين الداخليين بالتخاطب مع حاسب ما عن طريق الاسم فإن طلب الاتصال سوف يصل إلى مخدّم الأسماء الداخلية الذي يقوم بدوره بالتحقق من الطرف الآخر المطلـوب الاتصـال معه. فإذا كان الطرف الآخر محطةً داخليـةً فإنـه يقـوم بوصـل الطرفـين ويسـتجيب لطلـب الاتصـال

استجابةً سليمة. أمّا إذا كان الطرف الآخر محطةً خارجيـةً، فسـوف يقـوم مخـدّم الأسمـاء الداخليـة بتحويل الطلب إلى مخدّم الأسماء الخارجية الذي يقوم عندها بأداء المهمة. وبذلك نحقق أمن الأسمـاء الداخلية بعزلها عن المحيط الخارجي، حيـث يتصـل المسـتخدمون الخـارجيون مـع مخـدّم الأسمـاء الخارجية فقط، وهذا المخدّم لا يملك أية معلومة عن المحطات الداخلية لأنه لا يملك لائحة بالأسماء الداخلية، ومـن ثـم فإنـه سيسـتجيب لطلـب المسـتخدم الخـارجي برسـالة خطأ إذا كـان المسـتخدم الخارجي قد طلب أحد الأسماء الداخلية. لكن إعداد مخدّمي أسماء منفصلين مكلف إلى حد ما إضافةً إلى أنه قد يعرقل بعض الاتصالات. ولا يتفق الخبراء على أهمية هذه الطريقة، ولكنـهم يتفقـون تمامـاً على أن إخفاء الإنترانت إخفاءً بسيطاً لا يحقق الحماية الكاملة لها.

حماية اسم الموقع من ملف سجل الدخول على المواقع الأخرى

عندما تقوم إحدى المحطات بالاتصال مع مخدّم الوب فإنها تقوم بتسجيله في ملف تسجيل الدخـول الخاص بها (Logfile). وفي بعض المواقع ـ بالصدفة أو عن طريـق العمـد ـ تكـون هـذه الملفـات قابلـة للقراءة على الإنترنت، وعند استخدام مخدّم الوب (الذي نريد إخفاءه) للاستعراض علـى الإنـترنت، فمن المكن أن يدخل في إحدى هذه الملفات العامة، ومن ثـم قـد يدخـل اسمـه في فـهارس محركـات البحث. ومن الطبيعي أن يقوم كل مخترق بالاتصال بمحركات بحث كبيرة للحصول على اسم الشركة وذلك بالبحث عن أسماء غريبة (في حال افتراضه استخدام تقنية أسماء صعبة التخمين).

وتتكرر الحالة نفسها عند إرسال البريد الإلكتروني إلى قوائم البريد أو عند اسـتخدام Usenet، حيـث أن هذه المواقع مفهرسة أيضاً على الوب، الأمر الذي يجعل الفرصة سانحة للبحث عـن اسـم الشـركة في محرك بحث كبير.

والطريقة الوحيدة الناجحة في الإبقاء على أسماء المخدّمـات مخفيـةً عـن مسـتخدمي الإنـترنت، هـي ببساطة عدم استخدام هذه المخدّمات للنفاذ إلى الإنترنت.

4-3-3 أخطار سياسة التمويه

توجد حالياً برمجيات متعددة ومتاحة عبر شبكة الإنترنت يمكنها أن تبحث عن بوابات مفتوحة في موقع ما أو عدة مواقع. ولسوء الحظ فإن هذه البرمجيات التي تعتمد على عمليات مسح البوابات متاحة على الإنترنت في عدة مواقع ويمكنها أن تعمل بسرعة جيدة. وغالباً ما يستخدم المخترقون هذه البرمجيات لمسح بوابات البروتوكول TCP/IP في موقع مضيف لإيجاد المخدّمات المختبئة في هذا الموقع.

لكن هذه البرمجيات نفسها والتي تعتبر صديقاً أو حليفاً للمخترق يمكن أن تُستخدم من قبل مدير شبكة الإنترانت للقيام بعمليات مسح للتحقق من المخدّمات غير المسموح لها بالعمل في الشبكة والتي قد تسبب مشاكل أمنية، ويمكن الحصول على برمجيات مسح البوابات من مواقع مختلفة في شبكة الإنترنت ومنها ماسح البوابات "strobe" من الموقع ftp://suburbia.net/pub و "netcat" من الموقع ftp://avion.org /src/ hacks.

ومن الممكن التقاط كل من يشغل برمجيات مسح البوابات بإعداد بعض البرمجيات لخداع هؤلاء الأشخاص. كما يمكن إعداد مخدّمات مزيفة لتسجل كل شخص يقيم اتصالاً معها إضافةً إلى تحديد مكان هذا الشخص، وبتحليل هذه الاتصالات عبر المخدمات قد تتمكن الإنترانت من كشف وجود اعتداء قبل حدوثه.

يمكن استخدام مجموعة البرمجيات TCP Wrappers التي يمكن استقدامها من الموقع ftp://ftp.win.tue.n1/pub/security، حيث تعمل هذه البرمجيات وما يشابهها على التحقق من كل اتصال قبل إشراك المخدّم في هذا الاتصال. فعلى سبيل المثال يمكن إعداد هذه البرمجيات لتعمل مع المخدّم httpd، ويصبح بالإمكان الكشف عن عناوين IP التي أقامت الاتصال مع الشبكة، ومن ثم تقوم البرمجيات بالتحقق من أن المتصل هو صاحب العنوان IP الحقيقي، وأنه لا توجد عملية تزوير في العنوان IP، وعندها تقرر البرمجيات قبول أو رفض الاتصال. وفي حال قبول الاتصال يجري وصله مع مخدّم الوب على نحوٍ طبيعي، كما يوضّح ذلك الشكل (4-1).

كما يمكن أن تستخدم برمجيات TCP Wrappers لإعداد مخدّمات مزيفة، أو لإرسال البريد الإلكتروني، أو إرسال المعلومات إلى طابعة، أو إرسال صفحة وب إلى إدارة الشبكة إذا ما حاول أحدهم الاتصال ببوابة "مفخّخة".



بعد انتهاء التحقق

المخدّم ——— الزبون

الشكل (4-1): برمجيات TCP Wrappers

4-4 استخدام مخدّم الوب في الحماية

إذا كان إخفاء اسم الموقع لا يعتبر إجراءً أمنياً كافياً، فما هي إذن مقاييس الدفاع الأفضل المتاحة ؟ الجواب هو أن معظم مخدّمات الوب تقدم تقنية أساسية في الحماية تدعى التحكم بالنفاذ.

يمكن استخدام هذه التقنية لتعريف مجال من عناوين IP يُسمح لها باستقدام الملفات من مخدّم الوب، وتسمح معظم مخدّمات الوب بتحديد اسم المستخدم وكلمة السر قبل إرسال أي مستند.

وهذه الطريقة أقوى وأكثر فاعلية من الطرق السابقة في حماية مخدّم الوب من سوء الاستخدام من قبل المتطفلين، وعند استخدام هذه الطريقة هناك أحد النموذجين التاليين للسياسة الأمنية (المذكورين سابقاً):

- *كل ما هو غير مسموح ممنوع*، وهذا يعني أنه يجب البدء بمنع كل شخص من النفاذ إلى المخدم، والسماح بنفاذ مجموعة من الحواسيب المحددة فقط. يجري ذلك عادةً بوضع "*" أو all في حقل منع النفاذ ووضع رقم الشبكة المحلية في حقل السماح.

- *كل ما هو غير ممنوع مسموح* (وهي سياسة سيئة)، وهذا يعني السماح لأي شخص بالنفاذ إلى المخدّم ومنع بعض المواقع المحددة من النفاذ. وهذا يمكن أن يطبق بوضع '*' أو all في حقل السماح وسرد أسماء المواقع غير المرغوب بنفاذها في حقل المنع.

يتفق معظم خبراء أمن الشبكات بأن النموذج الأول هو النموذج الأكثر أمناً للشبكة، وذلك لأنه يقوم بمنع كل شيء والسماح فقط بما هو مطلوب. ويوفر هذا النموذج الأمني لمدير الشبكة إمكانية سيطرة أكبر على موارد الشبكة وعلى مستخدميها. في حين لا يوفر النموذج الثاني هذه الإمكانية لإدارة الشبكة إذ أنه يقدم لها طيفاً واسعاً جداً من المستخدمين القادرين على استثمار موارد الشبكة، بينما تحدّد لائحة المنع المحدودة المستخدمين والجهاتِ غير المسموح لهم بالنفاذ إلى الشبكة.

ومن الجدير بالذكر أن استخدام أمن مخدّم الوب قد يمنع أي متطفل خارجي من الحصول على معلومات من الشبكة عن طريق مخدّم الوب فقط، فهو يشكل طبقة حماية ضد المستخدمين خارج الشبكة ولكن هذه الحماية تقتصر على خدمة الوب، وتبقى حماية الشبكة من الاختراق بطرق أخرى من مهام أنظمة حماية أخرى سنذكرها لاحقاً.

4-4-1 المنع بواسطة عنوان IP

يجري تزويد مخدّم الوب عادةً بلائحة تحكم بالنفاذ إلى الشبكة، وهذه اللائحة تتضمن عناوين IP التي يقوم مخدّم الوب بالتعرف عليها والسماح لها بالنفاذ وباستعراض الملفات أو الأشكال عن طريق مخدّم الوب. وتُبنى لائحة التحكم بالنفاذ وفقاً لنموذج السياسة الأمنية المتبع في الشبكة حيث تتكون هذه اللائحة من حقول منع وحقول سماحية لتعريف عناوين IP الممنوعة من النفاذ والعناوين المسموح لها بالنفاذ إلى مخدّم الوب. ويقوم المخدّم بمقارنة عناوين طلبات الاتصال مع العناوين الموجودة في لائحة التحكم، ليقوم بعدها بقبول الاتصال أو رفضه وفقاً لحقول المنع والسماحية.

عند استخدام Apache مثلاً يجري بناء لائحة التحكم بالنفاذ الخاصة به لتحقيق منع نفاذ عناوين IP محددة وفقاً لما يلي:

تُكتب أوامر المنع في الملف access.cfg ويوجد هذا الملف عادةً في المجلد httpd/conf، وتجب كتابة أوامر المنع على النحو التالي:

```
<Limit>
	order deny, allow
	Deny
	Allow	123.123.123.
</Limit>
```

ومن الواضح أن هذه الأوامر تمنع كل الأشخاص من النفاذ إلى المخدم وذلك باستخدام '*' كما أشرنا سابقاً، وتسمح للعناوين IP التي من الشكل *.123.123.123 فقط بالنفاذ إلى هذا المخدم.

أمّا عند استخدام منع النفاذ بواسطة عناوين IP إلى مخدّم الوب باستخدام المخدّم Netware، فتكتب أوامر المنع بنفس السياق المستخدم في Apache، ولكنها تكتب هذه المرة في الملف ACSESS.CFG الموجود في المجلد \WEB\CONFIG.

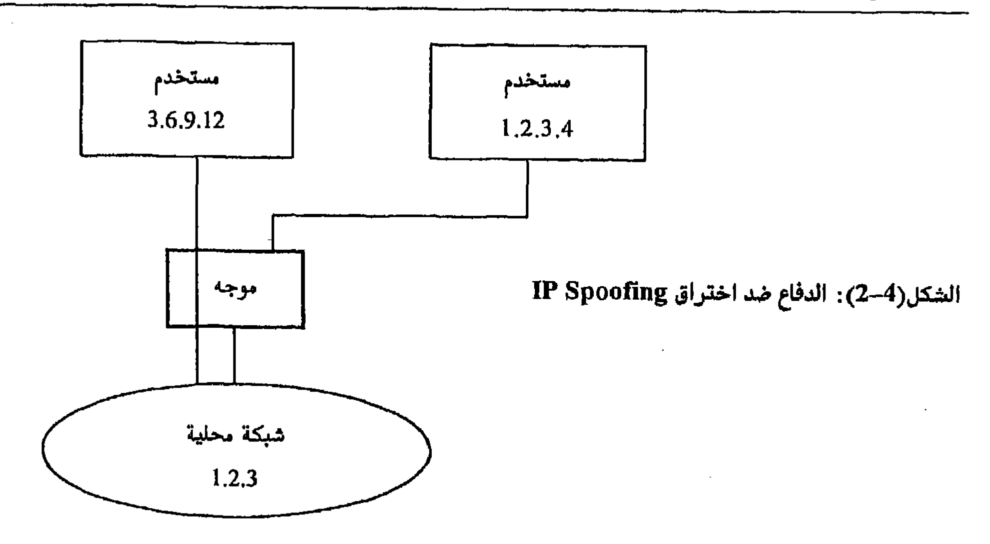
ومن أجل مخدّم الوب Netscape تبنى لائحة التحكم بالنفاذ باستخدام صفحة إدارة المخدم (Server Manager Page)، ومن ثم تُحدّد صفحة الإدارة (Administration Page) بواسطة المستعرض، ثم يجري اختيار الوصلة تحت التحكم بالنفاذ والمسماة تحديد النفاذ لعناوين محددة (Restrict Access from Certain Addresses)، مما يؤدي إلى إنشاء صفحة جديدة. يجري تحديد المورد المرغوب حمايته في هذه الصفحة وتوضع الإشارة '*' لحماية المخدّم الداخلي، ومن ثم تُدخل عناوين IP المحددة التي سيسمح لها بالنفاذ، وتكون هذه العناوين عادةً مؤلفة في القسم الأول منها من عنوان الشبكة المحلية متبوعاً بإشارة '*'.

فعلى سبيل المثال إذا كان عنوان IP للشبكة المحلية هو 123.123.123 فإن وضع العنوان *.123.123.123 في الحقل الخاص بالسماحية سوف يمكّن كل مستخدمي الشبكة المحلية الداخليين من النفاذ إلى مخدّم الوب، أما إشارة '*' في حقل المنع فسوف تؤدي إلى منع كل العناوين المخالفة للعناوين المسموح لها من النفاذ إلى مخدّم الوب.

ومن الجدير بالذكر أنه يمكن أيضاً استخدام برمجيات TCP Wrapper للحد من النفاذ إلى مخدّم الوب وذلك باستخدام مجال عناوين IP الممنوعة من النفاذ إلى المخدّم. تقدم هذه البرمجيات إمكانية إرسال رسالة خطأ للمستخدمين الخارجيين الذين يحاولون النفاذ بطريقة غير شرعية إلى مخدّم الوب، إضافةً إلى تنبيه الشبكة بخصوص هذه المحاولة والدلالة على مكان وجود المخدّم الخارجي الحقيقي الذي قام بمحاولة الاختراق.

4-4-2 تزوير عنوان IP

يُعتبر الحد من النفاذ إلى الإنترانت على أساس العناوين IP بدايةً جيدة لتحقيق حماية أمنية فعالة للإنترانت. وتبقى هذه الحماية متعلقة بالمزايا الأمنية التي يقدمها البروتوكول IP، فهذا البروتوكول قد صمّم بالأساس ليكون بروتوكولاً سهل الاستخدام، لذلك فهو يعتبر غير آمن عموماً. إذ يسمح هذا البروتوكول للمخترقين بإمكانية تزوير العناوين IP التي يستخدمونها، وذلك بالتنكر على هيئة مواقع أخرى قد تكون قادرة على النفاذ إلى الإنترنت. وهكذا يجري تحقيق اختراق قد يكون مدمراً بواسطة خدعة بسيطة، ويُسمى هذا التنكر بـ IP Spoofing. يمكن معالجة الخطر الناجم عن IP spoofing باستخدام لائحة التحكم بالنفاذ في الموجهات (سنتحدث عنها لاحقاً)، حيث يمكن استخدام الموجهات لمنع أي موقع على الإنترنت من استخدام عنوان IP داخلي. يوضّح الشكل (4-2) هذه العملية، وباستخدام هذه الطريقة لن تصل الطرود المرسلة من الخارج والتي تحمل عناوين داخلية إلى مخدّم الوب، لذا لا حاجة للقلق حيالها.



الشكل(4-2): الدفاع ضد اختراق **IP Spoofing**

لكن الحل السابق يبقى غير نافع إذا كانت هناك شركتان تتشاركان على مخدّم الوب عبر شبكة الإنترنت، فعندها سوف يقوم المخترق بالتظاهر أنه من الشركة الأخرى !

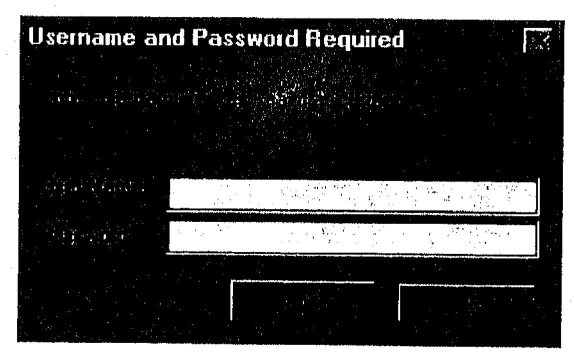
4-4-3 التحقق من الهوية

كما ذكرنا فإن البدء بحماية مواقع الإنترانت باستخدام عناوين IP تشكل بداية طيبة في بناء نظام أمني جيد، ولكنها لا تحقق الحماية الشاملة لموقع الوب.

يتشارك العديد من المستخدمين في كثير من الأحيان على حاسوب وحيد، وقد يكون المطلوب هو السماح لمستخدم وحيد بالنفاذ إلى الإنترانت. وقد يقوم هؤلاء المستخدمون بالاستفادة من مزوّد خدمة إنترنت ISP لتحقيق النفاذ إلى الإنترانت من خارج مكاتبهم، إذ قد تسمح خدمات ISP للعديد من الأشخاص بتحقيق النفاذ من خلال حاسوب وحيد، وتسمح لهم بالتشارك على عنوان IP وحيد عبر الشبكة. وهذا من شأنه أن يؤدي في بعض الأحيان إلى كارثة أمنية تسمح باختراقات لا تحصى لأنظمة الحماية القائمة أساساً على عناوين IP لاتخاذ قرارات المنع أو السماح بالنفاذ إلى الإنترانت. ويقتضي تجنب هذه المخاطر بضرورة استخدام أسماء وكلمات سر تخص المستخدمين المسموح لهم بالنفاذ إلى الإنترانت بالإضافة إلى الحماية باستخدام عناوين IP.

تسمح معظم مخدّمات الوب بتقنية بسيطة في التحقق من الهوية باستخدام أسماء المستخدمين وكلمات السر، فعندما يطلب المستخدم إحدى الصفحات المحمية فإنه سوف يتخاطب مع صندوق حوار يطلب منه اسمه وكلمة سره، وبعد التأكد من صحة الاسم وكلمة السر يُرسل المستند إلى المستخدم. وعند حدوث خطأ في كتابة الاسم أو كلمة السر تظهر رسالة خطأ للمستخدم، ويُمنع من الاطلاع على المستند. ويحتاج المستخدمون عادةً إلى إثبات هويتهم مرة واحدة في كل موقع أو في كل قسم، باستخدام الاسم وكلمة السر الخاصتين بكل منهم. يوضح الشكل (4-3) صندوق حوار كلمة السر. وتقوم برامج الزبون بتخزين اسم المستخدم وكلمة السر من أجل كل مجال أثناء كل جلسة اتصال، فلا يضطر المستخدم إلى إدخال هذه المعلومات إلا مرة واحدة.

ويعتبر البروتوكول HTTP نفسه من إحدى المشاكل التي تواجه نظام الحماية باستخدام أسماء المستخدمين وكلمات السر، حيث أنه يرسل النصوص بدون ترميزها، مما يسمح لأي شخص يمتلك جهاز محلل الشبكة (Snuffer) ويقوم بالتجسس على الشبكة بتحديد الملفات المنقولة ومعرفة اسم المستخدم وكلمة السر. ولمعالجة خطر هذه الأجهزة يجب استخدام النسخة الآمنة من البروتوكولات (S-HTTP, SSL) أو استخدام خط نقل مشفر.



الشكل (4-3) صندوق حوار اسم المستخدم وكلمة السر

ملاحظة

من الجدير بالذكر أن استخدام مزايا الحماية التي يقدمها مخدّم الوب سوف يؤدي إلى الحد من النفاذ إلى الملفات التي يمكن الحصول عليها بواسطة البروتوكول HTTP فقط. ويجب بالطبع حماية الطرق الأخرى المتبعة في تبادل الملفات مثلاً استخدام الحساب العام (Anonymous) في بروتوكول FTP.

4-4-4 إعداد تقنية التحقق من الهوية

سنعرض فيما يلي كيفية إعداد تقنية التحقق من الهوية على بعض مخدّمات الوب الشهيرة:

Apache

يتطلب تحقيق هذه التقنية في Apache إما تحرير موجه المجلد (Directory Directive) في الملف access.cfg، أو كتابة الملف htaccess ضمن المجلد المرادة حمايته. يكون شكل الأوامر التي تجب إضافتها إلى هذه الملفات كما يلي:

```
<Limit>
        require valid–user
        AuthName [Auth–domain]
        AuthType Basic
        AuthUserFile [user–file]
        AuthGroupFile [graup-file]
</Limit>
```

Netscape

تسمح مخدّمات Netscape أيضاً بالتحقق من الهويات وذلك بطريقة التحقق من أسماء المستخدمين وكلمات السر. ولتحقيق ذلك بواسطة هذه المخدّمات يجب أولاً اختيار مدير المخدّم (Server Manager)، ومن ثم اختيار الارتباط التشعبي (Restrict access to part of your server through authentication) تحت خيار التحكم بالنفاذ، وبعد اتباع التوجيهات وتعبئة الحقول المطلوبة يجب طبعاً إعادة تشغيل المخدّم، لتصبح هذه التغييرات فعالة.

NetWare

تسمح مخدّمات NetWare بالتحقق من الهويات بالاعتماد على تحرير بعض الملفات كما هي الحال في مخدّم Apache، أو بالاعتماد على NDS (Network Directory Service). ولكي يبدأ المخدّم

بالتحقق من الهويات يجب تحرير ملف النفاذ العام access.cfg، وقبل مؤثر المنع <Limit> </Limit> الخاص بمجلد البداية "Document Root"، تُضاف المؤثرات التالية:

- AuthType Basic: وتحدد نوعية التحقق المطلوبة.
- AuthName [name]: اسم يحدد كلمة السر التي يجب إدخالها.
- AuthUserName [file name]: ويحدد اسم الملف الذي يحوي كلمات السر المشفّرة.

وضمن مؤثر Limit تجب كتابة المؤثر Require، ليحدّد المخدّم المستخدمين المسموح لهم بالنفاذ إلى هذا المجلد، حيث نكتب قائمة بأسماء المستخدمين أو نكتب valid-user، وفي الحالة الأخيرة فإن أي مستخدم يستطيع النفاذ إذا كان اسمه موجوداً في الملف AuthUserFile بشرط أن يُدخل كلمة السر الصحيحة. أما الملف المشفّر الذي يحوي كلمات السر فيمكن بناؤه باستخدام التعليمة pwgen، وتأخذ هذه التعليمة اسم ملف الدخل واسم ملف الخرج كمتحولات لها، ويحوي ملف الدخل أسماء المستخدمين وكلمات السر بدون تشفير، مثلاً:

Rich : secret
Tom: quiet
Ali: ring

وبعد تنفيذ التعليمة pwgen، ننسخ الملف الناتج إلى مجلد جذر المخدّم (عادةً SYS:WEB)، كما يجب نسخ هذا الملف المشفّر على قرص مرن وحذفه من النظام، لضمان حمايته وعدم اكتشاف كلمات السر من قبل آخرين بالصدفة. أما في حال اختيار استخدام كلمات السر NDS، فيجب أولاً تشغيل البرنامج webmgr.exe لتحديد قيود النفاذ إلى المخدّم، ومن ثم نتبع الخطوات التالية:

1- أخذ الخيار File/seeet server لاختيار مجلد المخدم المطلوب.

2- اختيار مجلد جذر المخدّم المطلوب.

3- اختيار المجلد من اللائحة المنسدلة، ولحماية كامل المخدم الداخلي نختار \ .

4- اختيار Diretory Services من لائحة التحقق من الهويات (Authentication list).

5- كتابة اسم NDS الذي يتضمن غرض المستخدم الذي يجب أن يحصل على حق النفاذ.

6- اختيار اسم المستخدم.

7- اختيار إضافة (Add) لإضافة المستخدم إلى لائحة المستخدمين المسموح لهم بالنفاذ.

9- اختيار الحفظ Save ومن ثم إعادة التشغيل.

10- إدخال كلمة سر مخدّم الوب ثم اختيار موافق Ok لتأخذ التغييرات مفعولها.

Microsoft IIS

يمكن أيضاً تحقيق عملية التحقق من الهويات باستخدام Microsoft IIS، وذلك بفتح صندوق خصائص مخدّم الوب واختيار صفحة المخدّم، ثم اختيار الخيار الذي يدعم التحقق من الهويات بواسطة كلمات السر. ويؤدي هذا بالطبع إلى إجبار المستخدمين الراغبين بالنفاذ إلى المخدّم على كتابة أسمائهم وكلمات سرهم الصحيحة، ويجب أن تقابل هذه الأسماء حسابات صحيحة على الحاسب المشغل للنظام Microsoft IIS، أو في أي مجال NT قابل للنفاذ.

4-4-5 طرق نفاذ أخرى

تختلف أساليب المخترقين في النفاذ إلى شبكة الإنترانت، ولا تزال المعركة قائمة حتى الآن ما بين نظم الأمن المتبعة في الإنترانت، والتي تتطور تطوّراً متزايداً، والتقنيات التي يطورها المخترقون للنفاذ غير الشرعي إلى موارد الإنترانت. وبالرغم من كل الأساليب السابقة الممكن اتباعها في حماية مخدّم الوب، إلاّ أنه توجد طرق أخرى يستطيع فيها المخترقون الوصول إلى مخدّم الوب مهما كانت أنظمة حمايته شديدة التعقيد. وهناك طرق حماية أخرى أكثر أمناً تتمثل في وضع مخدّمات الإنترانت خلف ما يُسمى الجدار الناري (Fire Wall)، واستخدام الموجهات المرشحة (Filtering Routers)، ومخدّمات الوكيل (Proxy Servers)، وهذا من شأنه أن يصدّ كل محاولات النفاذ غير المرغوبة إلى مخدّمات الإنترانت.

ويجب ألا ننسى أن النمـوذج الأمـني الأكـثر نجاحـاً في صـدّ الاختراقـات الـتي تتعـرض لهـا شـبكة الإنترانت يتمثل في منع كل الاتصالات، والسماح فقط بالاتصالات الآمنة. وقد أصبح هذا النموذج هـو النموذج الوحيد المتبع في بناء نظام أمني للإنترانت غير قابل للاختراق.

5-4 الموجّهات المرشّحة

تُعتبر الموجّهات خط الدفاع الأول ضد النفاذ غير المسموح به إلى شبكات الإنترانت وذلك لكونها ممـراً إجبارياً يجب على المخترق سلوكه للوصول إلى موارد الإنترانت من الخارج، ويجب وضع الموجّـهات في المرتبة الأولى عند دراسة تصميم وبناء النظام الأمني لشبكة الإنترانت.

تقوم الموجّهات بفحص كل طرد وارد إلى الإنترانت أو خارج منها، ومن ثم توجّه الطـرود إلى العنـوان المطلوب وفق أفضل مسار، أي أنّ الموجهات تتحكم بنوعية واتجاه حركة سير المعطيات المسموح بـها عبر الشبكة، وتمتلك القرار الأول في عملية توجيه الطرود في الشبكة وإيقاف بعض الطـرود الـواردة أو الخارجة عبر شبكة الإنترانت.

وعند توظيف هذه الموجّهات في ترشـيح الطـرود العـابرة في الشـبكة فإنـها تسـمى عندئـذ بالموجّـهات المرشحة (Filtering Routers) أو بالموجّهات العارضة (Screening Routers).

وكما ذكرنا في الفصل الثـالث، فـإن كـل موجّـه يملـك جـدولاً للتوجيـه ويُبنـى ديناميكيـاً أو يدويـاً، وسنسمي هذا الجدول في الموجّهات المرشحة جدول الترشيح (Filtering Table)، إذ أنه يحتوي على عدة قواعد ناظمة لحركة سير المعطيات عبر الشبكة، وذلك بتحديد نوعية الطرود المسموح لها بالتنقل عبر الشبكة أو الطرود الواجب منعها.

تملك طرود المعلومات المتنقلة عبر الشبكة عدة مستويات من المعلومات، تحدد هذه المستويات نوعيـة الطرد من حيث المعطيـات الأساسـية المنقولـة، ومعلومـات حـول نـوع مصـدر الإنـترنت المسـتخدم في

تشكيلها (Telnet , FTP وغيرها)، وعناوين المرسل والمستقبل لهذه الطرود. وتستخدم الموجّهات المرشحة هذه المعلومات لتقييم القواعد الواجب تطبيقها على كل طرد.

عندما تمر الطرود عبر الموجّهات، يقوم الموجّه بفحص الطرد ومقارنته مع جدول الترشيح ومن ثم يقوم باتخاذ القرار للسماح بمرور هذا الطرد أو عدم السماح له بذلك. وتختلف القواعد المطبقة حسب جهة انتقال الطرود، إذ يمكن التمييز ما بين الطرود الواردة والطرود الخارجة من الشبكة، وهذا يعني إمكانية إعطاء المستخدمين داخل الإنترانت مستويات مختلفة في الحصول على الخدمات والمعطيات، وطبعاً منع الناس خارج الإنترانت من الحصول على موارد أو معطيات الإنترانت.

فقد يسمح الموجّه المرشّح، على سبيل المثال، لمستخدمي الإنترانت باستخدام Telnet، في حين يمنع أي مستخدم خارجي من استخدام Telnet عبر الإنترانت. فهو يستطيع منع مصادر محددة من العناوين من الوصول إلى الإنترانت، وهو كما ذكرنا (الموجّه المرشّح) قادر على التمييز ما بين المعطيات الداخلة والخارجة عبر البوابات، فإذا استطاع أحد تزوير أحد عناوين الشبكة الداخلية محاولاً إظهار نفسه كمستخدم داخلي فإن الموجّه سيميز العنوان على أنه عنوان داخلي قادم من بوابة خارجية، وهذا الوضع يعني حصول عملية اختراق بالنسبة للموجّه، فيقوم الموجّه بصد الطرد وإهماله (الشكل 4-2).

4-5-1 كيفية عمل الموجّهات المرشّحة

يمكن لمدير الإنترانت أن ينظّم جدولاً يضم مجموعة القواعد التي تستخدمها الموجّهات المرشّحة لاتخاذ القرار حيال الطرود بتمريرها أو عدم تمريرها.

1- يجري إعداد قواعد مختلفة لكل من الطرود الواردة إلى الإنترانت عن طريق الموجّه والطرود المرسلة من قبل الإنترانت، مما يسمح للمستخدم الداخلي بالحصول على الخدمات الخارجية ومنع أي مستخدم إنترنت خارجي من الوصول إلى خدمات الإنترانت.

2- يقوم الموجّه بملاحقة الطرود التي لم يُسمح لها بالمرور من الإنترنت إلى الإنترانت، مما يدل على أن الإنترانت قد تعرضت للهجوم.

3- يفحص الموجّه معلومات ترويسة IP التي تغلف المعطيات، وترويسة طبقة النقل في كل طرد، ومن ثم يقوم بفحص ترويسة طبقة النقل ثم المعطيات، قبل السماح للطرود بالمرور.

4- يقوم الموجّه بقراءة العنوان في حقل المصدر في ترويسة الطرد IP، ومن ثم يقوم بمقارنة هذا العنوان مع لائحة العناوين المسموح لها بالمرور، وهذه اللائحة مدرجة في جدول الترشيح. ومن المهم أن يحوي هذا الجدول على الأقل عناوين IP التي تعتبر خطيرة وغير مسموح لها بالمرور إلى الإنترانت، أو أن يحوي فقط على عناوين IP المسموح لها بالمرور إلى الإنترانت. ويتعلق هذا بطبيعة السياسة الأمنية المتبعة: "كل ما هو غير مسموح ممنوع"، أو "كل ما هو غير ممنوع مسموح".

5- يمكن للموجّهات أن تطبق قواعد مختلفة على الشبكات الجزئية لأن هذه الشبكات قد تتطلب مستويات متفاوتة من الحماية. فالشبكة الجزئية التي تحتوي على معلومات مالية عالية الخصوصية، أو معلومات تخص موضوع التنافس يجب أن تكون محمية جداً، ويجب أن تطبق عليها قيود أمنية عالية المستوى. في حين قد تتطلب شبكة المهندسين قيوداً أقل على نشاطات النقل من وإلى الإنترانت بسبب طبيعة وظيفتها لها وأهمية تبادل المعلومات في هذا الإطار.

6- يستطيع الموجّه المرشّح السماح للمستخدمين بالحصول على خدمات الإنترنت، بينما يمنع الإنترنت من استخدام نفس الخدمات في الإنترانت. وتُستخدم هذه التقنية نفسها لمنع المستخدمين الداخلين من الوصول إلى المعلومات المحمية في شبكة الإنترانت. فعلى سبيل المثال يمكن السماح لموظف مالي باستخدام FTP، بينما نسقط الخدمة FTP التي تسمح لقسم الهندسة بالوصول إلى القسم المالي.

7- تكون بعض الخدمات أكثر خطورة من بعضها الآخر، فمثلاً، تُستخدم خدمة FTP لاستقدام الملفات وربما يجري إحضار ملفات تحتوي بعض الفيروسات، وخدمة Telnet وrloging تكون

غالباً مقيدةً بقواعد في جدول الترشيح. وتحدّد هذه القواعد نوعية هذه الخدمات باستخدام رقم البوابة المصدر ورقم البوابة الهدف. نجد مثلاً في البروتوكول TCP أو UDP رقم بوابة Telnet هو 23 ورقم بوابة rlogin هو 523. يبين الجدول التالي المعلومات الواجب اعتبارها في الطرود لتحديد نوعية الاتصال في خدمة Telnet، وبناء على تحقق معلومات أحد الأسطر في الجدول يمكننا الجزم بنوع الخدمات المنقولة عبر الطرود.

مصدر الاتصال	جهة الطرد	عنوان المصدر	عنوان الهدف	بوابة المصدر	بوابة الهدف
داخلي	إلى الخارج	داخلي	خارجي	p	23
داخلي	إلى الداخل	خارجي	داخلي	23	p
خارجي	إلى الداخل	خارجي	داخلي	q	23
خارجي	إلى الخارج	داخلي	خارجي	23	q

الجدول (4-1): معلومات ترويسة الطرود في وصلات Telnet الداخلة والخارجة

إن الرقم 23 هو رقم بوابة Telnet المعيارية على المخدّم، أمّا الرمزان p و q فيدلان على أرقام البوابات المستخدمة من جهة الزبون.

8- تُعتبر طريقة خداع العنوان (Address Spoofing) طريقةً شائعةً للهجوم على شبكة الإنترانت. وفي هذه الطريقة يستطيع أحد المستخدمين خارج الإنترانت تقليد عنوان مصدر يظهر للموجّه وكأنه عنوان مصدر داخلي في الإنترانت، وبذلك يحاول المقلد خداع الموجّه المرشّح ليستطيع الوصول إلى شبكة الإنترانت بحرية مستخدم داخلي، ومن ثم يجري إرسال ملفات خاصة إلى خارج الإنترانت إذا نجحت هذه الخدعة واقتنع الموجّه بعنوان IP المزيف.

9- يجب أن يمتلك الموجّه المرشّح تقنية مضادة لطريقة خداع العنوان، فيجب وضع قاعدة أمنية تمكن الموجّه من النظر في ترويسة IP لكل طرد وارد إلى شبكة الإنترانت على حدة، وعدم الخلط

بين الطرود الواردة والطرود الخارجة للتمييز بين عنوان IP للمصدر الداخلي (ويكون بالطبع في طرد خارج من الشبكة أو يتنقل عبر الشبكة)، وبين عنوان IP كمصدر داخلي مزيف وارد من خارج الشبكة.

4-6 مخدّمات الوكيل

يعتبر السماح للمستخدمين الداخليين في شبكة الإنترانت بالوصول مباشرة إلى مخدّمات وموارد شبكة الإنترنت أمراً غير مرغوب فيه من وجهة نظر النظام الأمني للإنترانت. فقد تسبب بعض الملفات المستقدمة من الإنترنت إتلاف ملفات حاسوب المستخدم الذي أجرى عملية الاستقدام إضافةً إلى ملفات أخرى في الإنترانت. كما أنه يصبح من الصعب، عند السماح لمستخدمي الإنترانت الداخليين بالنفاذ غير المقيد إلى الإنترنت، على إدارة الإنترانت أن تسيطر على كل عمليات الاختراق التي تستهدف السيطرة على حواسيب ومخدّمات الإنترانت.

يُعتبر استخدام مخدّمات الوكيل الحلُّ الأنسب والملائم لتلافي المشاكل السابقة. كما أن استخدام مخدّمات الوكيل يُوازن بين وظيفتين متباينتين وهما تزويد مستخدمي الإنترانت الداخليين بخدمة النفاذ السهل إلى شبكة الإنترنت من جهة، والمحافظة على أمن الإنترانت من جهة أخرى. فعندما يرغب أي مستخدم داخلي بالحصول على خدمة من شبكة الإنترنت فهو في الواقع لا يتصل مباشرة مع الإنترنت بل مع مخدّم وكيل. فعلى سبيل المثال عند رغبة المستخدم بالحصول على صفحة وب فإن المستخدم يتصل بالمخدّم الوكيل، الذي يقوم بدوره بالاتصال مع مخدّم الوب في شبكة الإنترنت ومخدّمات الإنترنت، وتقوم مخدّمات الوكيل بتسجيل كل الاتصالات التي تقوم بها مع شبكة الإنترانت، بحيث يستطيع مدراء الإنترانت الإشراف على هذه العملية وفحص جميع الثغرات التي قد تتعرض للهجوم من قبل المخترقين.

كما تستطيع مخدّمات الوكيل تقديم خدمة عظيمة لأمن الإنترانت، وذلك بأن تخبئ بعض صفحات الوب القادمة من الإنترنت في ذاكرتها، والتي تشكّل الصفحات الأكثر طلباً من قبل المستخدمين

الداخليين، وهذه الخدمة تقلص عدد الاتصالات مع الإنترنت. فعندما يطلب أحد المستخدمين صفحة وب من المخدم الوكيل فإنه قد يحصل عليها دون الحاجة للاتصال مع الإنترنت لأنها قد تكون موجودة في الذاكرة. وتصبح تلبية طلبات المستخدم عملية داخلية لا تستدعي الخروج من الإنترانت، وبما أن الاتصالات في الإنترانت أسرع منها في الإنترنت، فإن المستخدم يحصل على تجاوب وعرض سريعين لصفحات الوب ولموارد أخرى على الإنترنت، إضافةً إلى الفائدة الأمنية التي تحصل عليها الإنترانت.

ويمكن تزويد الإنترانت بأكثر من مخدّم وكيل واحد، كما أنه يمكن تحديد مخدّمات وكيلة منفصلة لكل من الوب، وTelnet، وFTP، وخدمات شبكة الإنترنت الأخرى. كما أنه من الممكن أيضاً وجود خدمات قد لا تتصل بمخدّمات وكيلة.

وعندما تصبح هناك خدمات إنترنت جديدة، فمن المحتمل أن لا تستخدم مخدّمات الوكيل في بادئ الأمر، حيث سيجري التعامل المباشر مع هذه الخدمات ريثما تتطور تكنولوجيا مخدّمات وكيلة حديثة ومتوافقة معها.

كما يتوجب دائماً على برمجيات الزبون الخاصة بمخدّمات الوكيل أن تُستخدم بانسجام مع المخدّمات الوكيلة المتاحة، وهذا من شأنه أن يتسبب في بعض المشاكل أحياناً، إذ لا تملك جميع نظم العمل المتوفرة في الإنترانت برمجيات زبون لكل خدمات الإنترنت المطلوبة. ومن المشاكل الأخرى المحتملة أن تحتاج الإنترانت إلى برمجيات زبون غير معيارية، وهي ستكون بالطبع صعبة الاستخدام. يكون في هذه الحالة من المفضل استخدام البرمجيات المعيارية، مثل Netscape Navigator، حيث يجري إعداد هذه البرمجيات للتعامل مع المخدّم الوكيل، وعندها سيقوم كل من البرمجية والمخدّم بأداء بقية العمل.

4-6-1 عمل مخدّمات الوكيل

تشكّل مخدّمات الوكيل جزءاً متكاملاً في العديد من نظم أمن الإنترانت، ومن الممكن تطبيق قواعد تمرير المعلومات على هذه المخدّمات لتؤدي عملاً مشابهاً للموجّهات المرشّحة.

يجري بناء النظام الأمني الواجب اتباعه من قبل المخدّم الوكيل بتحديد نوعية الخدمات التي يجب أن يمررها هذا المخدّم، والخدمات الأخرى التي يجب أن لا يمررها. ويجري إعداد المنع والسماحية من قبل مدراء الإنترانت، وذلك بعد إعداد برمجيات منفصلة ومحددة لكل نوع من خدمات الإنترنت.

وتعمل مخدّمات الوكيل كما يلي:

1- عندما يقوم حاسوب شخصي على الإنترانت بطلب خارجي لخدمة من الإنترنت فإن هذا الحاسوب الداخلي يتصل بمخدّم وكيل، ويقوم هذا المخدّم بالاتصال مع مخدّم الإنترنت بدلاً من الحاسوب، ومن ثم يزود هذا الحاسوب بالخدمة المطلوبة بعد حصوله عليها من الإنترنت.

2- يسجل المخدّم الوكيل كل حركات المرور الحاصلة على الإنترانت والإنترنت. فعلى سبيل المثال يستطيع المخدّم الوكيل الخاص بـ Telnet تتبع كل حرف مدخل في جلسة Telnet على الإنترانت، كما أنه يستطيع ملاحقة كيفية استجابة المخدّم الخارجي على الإنترنت للأحرف المدخلة. ويقوم المخدّم الوكيل بتسجيل عنوان IP من أجل كل اتصال، مع تاريخ وزمن الدخول، والعنوان URL، وعدد الثمانيات المستقدمة،.... وتُستخدم هذه المعلومات من قبل إدارة الشبكة لتحليل أي نفاذ للحصول على خدمة من قبل العاملين.

3- يتوجب على بعض مخدّمات الوكيل العمل مع برامج زبون خاصة. ومن الشائع كما ذكرنا استخدام البرامج المعيارية مثل Netscape Navigator مع مخدّمات الوكيل، وهذه البرمجيات يجب أن تكون مهيئة للعمل مع مخدّمات الوكيل، عندئذ يستطيع موظف الإنترانت استخدام برمجية الزبون بسهولة أكبر، وهذه البرمجية هي التي تسمح بالذهاب إلى المخدم الوكيل للحصول على المعلومات بدلاً من الذهاب إلى الإنترنت.

4- يمكن إعداد مخدّمات الوكيل من أجل الخدمة FTP للسماح بنقل الملفات المرسلة من الإنترنت إلى الإنترانت، ولإيقاف الملفات المرسلة من الإنترانت إلى الإنترنت، أو بالعكس. ويتمكن مدراء الإنترانت في هذه الحالة من إيقاف أي مستخدم من خارج المؤسسة يحاول استقدام معلومات حيوية تخص المؤسسة، أمّا في الحالة العكسية فيجري منع استقدام ملفات قد تحوي فيروسات من بعض المواقع السيئة في الإنترنت.

5- تستخدم أيضاً مخدّمات الوكيل لتسريع بعض خدمات الإنترنت، وذلك بالاحتفاظ بأكثر المعلومات تواتراً (التي يتزايد الطلب عليها من قبل المستخدمين الداخليين) في ذاكرتها. وفي هذه الحالة يستطيع المستخدم الداخلي الحصول على الخدمة بسرعة أكبر بسبب استخدام خطوط شبكة الإنترانت فقط دون الحاجة إلى الخروج إلى شبكة الإنترنت التي تكون خطوطها عادة ذات سرعة أقل.

4-7 الجدار الناري

الجدار الناري (Firewall) هو نظام أو مجموعة أنظمة تجبر شبكتين مختلفتين على اتباع سياسة محددة في تبادل المعطيات بينهما، حيث يلعب هذا الجدار دور العازل بين الشبكتين ويؤمن حماية حركة المعطيات في كل شبكة دون أن تستطيع الشبكة الأخرى الوصول إلى هذه المعلومات كما أنه يقوم بتنظيم حركة المعطيات المتبادلة بين الشبكتين أثناء فترة الاتصال.

وبالرغم من أنه يمكن بناء الجدار الناري بين أي شبكتين، لكن الاستخدام الشائع له هو في عزل شبكة الإنترانت عن شبكة الإنترنت خصوصاً. إذ يستطيع حماية المعلومات في شبكة الإنترانت من العديد من الاختراقات التي قد تحدث نتيجة الوصل مع الإنترنت، حيث أنه يقوم بعملية فرز وتحقق من كافة الطرود المتبادلة بين الشبكتين، ومن ثم يقوم بعملية انتقاء لتحديد نوعية الطرود والبروتوكولات المسموح لها بالمرور عبر الإنترانت.

والجدار الناري غير قادر على حل جميع مشاكل الأمن المتعلقة بشبكة الإنترانت ولكنه يعتبر من أقوى الأنظمة المستخدمة في بناء أنظمة الحماية المطلوبة. ولتأمين حماية أمن معلومات الإنترانت بفعّالية فإنه من الضروري تدعيم تقنية الجدار الناري بعدة أنظمة أخرى مساعدة كتلك التي جرى استعراضها في هذا الفصل حتى الآن.

يمكن تمييز نوعين من أنظمة الجدار الناري وذلك بحسب نوعية الحماية التي تضمنها للشبكة، وهذان النوعان هما:

- الجدار الناري في طبقة الشبكة (Network-Level Firewalls).
- الجدار الناري في طبقة التطبيق (Application-Level Firewalls).

يقدّم كل من النوعين السابقين مصادر حماية فعّالة ومختلفة، ولكل منهما نقاط ضعف قد تؤدي إلى حدوث بعض الاختراقات، لذلك يفضّل عند بناء نظام الجدار الناري للإنترانت أن نستخدم تركيباً يتضمن كلا النوعين السابقين وذلك تبعاً لمتطلبات الأمن المرغوبة.

4-7-1 الجدار الناري في سوية الشبكة

يقوم هذا النظام بفحص ترويسة IP للطرود المتبادلة بين شبكتي الإنترانت والإنترنت، ويتخذ القرار السماح بمرور هذه الطرود أو بمنعها تبعاً للسياسة الأمنية الموضوعة من قبل مدراء الإنترانت. ولا يقوم الجدار الناري في هذه الطبقة بفحص كتلة المعطيات المحمولة في الطرود وهو ليس معنياً بفهم ما يحدث أثناء تبادل هذه المعطيات، وإنما يقوم فقط بعملية ترشيح لهذه الطرود بناءً على العناوين IP التي تحملها وعلى رقم بوابة التطبيق. من أبسط أشكال هذا الجدار هو الموجّهات المرشّحة التي استعرضناها سابقاً، والتي تقوم باتخاذ قرارات السماح أو المنع بمرور الطرود عبر الإنترانت بعد مقارنة العناوين IP التي تحملها مع العناوين الموجودة في جداول السماح بالنفاذ الموضوعة من قبل إدارة الشبكة.

يمتاز الجدار الناري في طبقة الشبكة بسرعته الكبيرة في العمل حيث يفحص ترويسة الطرود IP العابرة، وهو شفاف لا يقوم بالتدخل في معطيات الطرود، ولا يحتاج المستخدم إلى تعلم أي أوامر خاصة لاستخدام هذا الجدار. وبما أنه يصل بين شبكتين مختلفتين فإنه يجب على الشبكتين استخدام مجالات عناوين IP مناسبة.

يمتاز الجدار الناري في سوية الشبكة بالنقاط التالية:

- سهل التشكيل والبناء.
- شفاف بالنسبة للمستخدم.
- سريع جداً.
- رخيص نسبياً.

بينما يعاني هذا الجدار من المشاكل التالية:

- تعتمد عمليات النفاذ على العناوين IP وأرقام البوابات فقط.
- يتطلب دراسة معمقة لمجال عناوين IP.
- احتمال التعرض لتزوير العناوين IP.

يستند الجدار الناري في طبقة الشبكة إلى سياسة أمنية محدّدة وموضوعة من قبل إدارة الشبكة، وتتمثل هذه السياسة بمجموعة من اللوائح الناظمة لعمليات المرور وتتضمن مجموعة القواعد التي يقوم الجدار الناري على أساسها بالسماح بمرور الطرود أو بمنعها. ونورد فيما يلي مثالاً عن هذه اللوائح:

قاعدة 1: السماح للبوابة 25 (E-Mail) بالنفاذ إلى لوائح البريد من قبل أي مستخدم.

قاعدة 2: السماح للبوابة 80 (WWW) بالنفاذ إلى مخدّم الوب الخارجي من قبل أي مستخدم.

قاعدة 3: السماح لمستخدمي الشبكة 123.243.123 بالنفاذ إلى البوابة 23 (Telnet).

قاعدة 4: عدم السماح بأي شيء آخر.

والسطر الأخير في اللائحة السابقة هو السطر الأهم حيث أنه يتوافق مع السياسة الأمنية "كل ما هو غير مسموح ممنوع". وتكون لائحة النفاذ أكثر تعقيداً من هذه اللائحة البسيطة طبعاً، ويزداد تعقيدها طرداً مع التشدد الأمني الواجب اتباعه في الشبكة.

تسمح بعض تشكيلات الجدار الناري بتعريف ما يجب فعله في حال عدم السماح بمرور أحد الطرود، وذلك بتنظيم تقارير أمنية ترفع إلى إدارة الشبكة وتستخدم لدراسة الطرود الواردة والمرسلة عبر الشبكة وتقييم الحالة الأمنية للشبكة، وذلك بهدف تعزيز القدرة على الاستجابة المباشرة ضد أي خطر.

يستخدم الجدار الناري في طبقة الشبكة برمجيات ترشيح الطرود التي تقوم بقبول أو رفض الطرود استناداً إلى العناوين IP وإلى رقم البوابة المستقبلة، حيث تقوم هذه البرمجيات بعمل مشابه لعمل الموجّهات المرشّحة وتستخدم في بناء العديد من تشكيلات الجدار الناري، ويمكن نسخ هذه البرمجيات من المواقع التالية:

IP Filter, ftp://coombs.anu.edu.au/pub/net/kernel

KarlBridge, ftp://ftp.net.ohio-state.edu/pub/kbridge

Screened, ftp://decuac.dec.com/pub/sources

وتدعم هذه البرمجيات العديد من بطاقات الشبكة، وهي متاحة كذلك على نظام التشغيل DOS ونظام التشغيل UNIX.

4-7-2 الجدار الناري في طبقة التطبيق

يُعتبر الجدار الناري في طبقة التطبيق نموذجاً أكثر أمناً من الجدار السابق حيث أنه يؤمن عزلاً أفضل بين الشبكة الداخلية والشبكة الخارجية، حيث يعتمد هذا النموذج هو على حاسوب مضيف مزّود ببطاقتي شبكة على جانبي الشبكة الداخلي والخارجي. وتعمل على هذا الحاسوب مجموعة من المخدّمات الوكيلة الخاصة بكل خدمة من خدمات الإنترنت، ويسمى هذا الحاسوب أحياناً البرجَ المضيف (Bastion Host)، ويمنع هذا البرج حركة النقل بين جانبي الشبكة، وبدلاً من تمرير المعطيات فإن الوكيل يقوم بنقل المعطيات ذهاباً وإياباً.

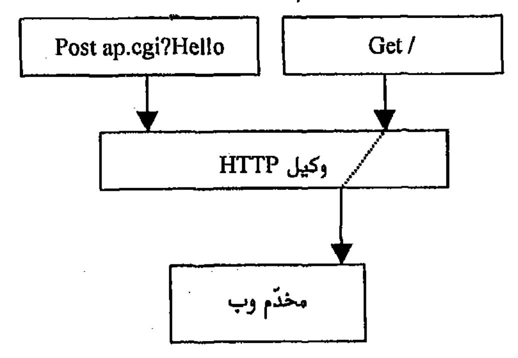
على اعتبار أن الجدار الناري في طبقة التطبيق يتعامل مع بروتوكـولات نقـل ذات مواصفـات مختلفـة فهو يحتاج إلى فهم كل بروتوكول على حدة، وذلك ليتمكن من القيام بالتحكم المطلوب بعمليات النفاذ إلى الإنترانت وتسجيل حركة النقل. فعلى سبيل المثال، يمكن إعداد مخدّم وكيـل مـن أجـل الخدمـة HTTP للسماح بالحصول على الصفحات فقط دون الصور، وهذا المخدّم يحدّ مـن عمليـات النفـاذ إلى الإنترنت عبر الخدمة HTTP، كما أنه من الممكن أن يجري إعداده لمنع تشغيل برمجيات CGI كمـا هو موضح بالشكل (4-5).

يمتاز الجدار الناري في طبقة التطبيق بالنقاط التالية:

- تحكم ممتاز بالنفاذ.
- تسجيل أفضل لعمليات المنع والسماح.
- يمكنه أن يتعامل مع مجالات عناوين IP محجوزة أو غير مسجلة.

بينما يعاني هذا الجدار من المشاكل التالية:

- صعب التنفيذ نوعاً ما.
- أداء منخفض مقارنة مع الجدار الناري في طبقة الشبكة.
- يحتاج كل بروتوكول إلى برمجيات خاصة به.
- غير شفاف دائماً بالنسبة للمستخدم.



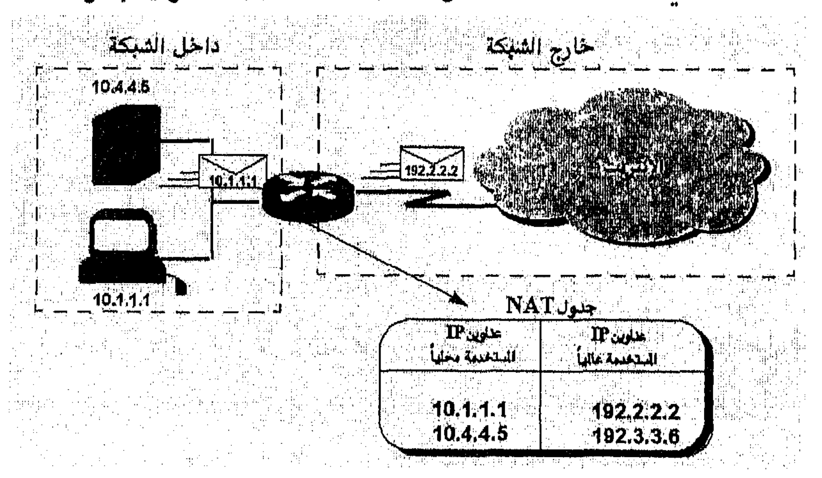
الشكل (4-5): السماح بالحصول على الملفات من المخدّم ومنع تنفيذ البرامج عليه

ترجمة العناوين

بما أن الجدار الناري في طبقة التطبيق يربط الرسائل المتبادلة عبر الشبكة بدلاً من تمرير حركة النقل، فإنه يستطيع القيام بدور مترجم عناوين الشبكة NAT (Network Addresses Translators)، وهي وظيفة بالغة الأهمية في الشبكات التي تعتمد على العنونة IP وخاصة تلك التي تستخدم مجالات عنونة غير مسجلة أو مجالات عنونة محجوزة.

لقد أدى النمو الانفجاري لشبكة الإنترنت إلى ضيق في مجالات العنونة IP، وهذا يعني عدم توفّر عناوين IP مسجلة كافية لكل الشبكات التي تستخدم البروتوكول IP. وتنصح الوثيقة RFC 1597 باستخدام مجالات عناوين IP غير القابلة للاستخدام على الإنترنت، إما لأنها محجوزة أو لأنها غير مسجلة، من أجل العنونة الداخلية في الشبكات المحلية، وقد أصبح من الضروري، لوصل هذه الشبكات الداخلية بالإنترنت، استخدام مترجمات عناوين الشبكة NATs لتحقق التوافق المطلوب مع العناوين IP المستخدمة عالمياً.

وعلى اعتبار أن تصميم الإنترنت قد جرى أصلاً بحيث يضمن عدم توجيه أي عملية نقل إلى أي مجال عناوين IP محجوز، فإن استخدام هذا النوع من المجالات في العنونة من أجل الشبكات الداخلية قد يساعد في تجنب عمليات الاختراق للشبكات الداخلية عن طريق الإنترنت.



الشكل (4-6): ترجمة العناوين NAT

يضمن الجدار الناري في طبقة التطبيق حماية إضافية لشبكة الإنترانت عند السماح باستخدام مجالات عنونة IP محجوزة، وهذه الميزة الأمنية ليست مجانية بالطبع، إذ يجب القيام بعملية ترجمة العناوين عند الاتصال مع الخارج.

المخدّم الوكيل

يعتمد الجدار الناري في طبقة التطبيق على مخدّمات الوكيل أيضاً، وهي تستطيع التعامل مع كل بروتوكول يقوم بعبور الجدار الناري، حيث تمتلك أغلب التطبيقات المشهورة برمجيات وكيل خاصة ومكتوبة لها خصيصاً.

فعلى سبيل المثال، قامت شركة TIS (Trusted Information Systems) بإصدار مجموعة برمجية تضم مخدّمات وكيل لكل من الأدوات التالية: HTTP, Xwindows, FTP, Telnet, rlogin.

يجب عند استعمال أحد هذه البروتوكولات في الإنترانت النظر في السياسة الأمنية لمعرفة فيما إذا كان استخدام هذا البروتوكول ضرورياً، حيث أن إمكانية السماح بتمرير هذا البروتوكول تمريراً آمناً عبر الجدار الناري لا يعني ضرورة السماح به عبر الشبكة.

وفي حال اضطررنا إلى استخدام بروتوكولات جديدة لم تكتب برمجيات وكيلة خاصة بها بعد، فيجب تمرير هذه البروتوكولات عبر الجدار الناري في طبقة الشبكة، أو عبر مخدّم وكيل عمومي، أو عبر يُسمى مرسل التطبيق.

مرسلات التطبيق

مرسلات التطبيق (Application Forwarders) هي نوع من الأدوات ذات الاستخدامات الطارئة بالنسبة لإدارة الجدار الناري، حيث أنها تستخدم ما يشبه المخدّم الوكيل لدعم التطبيقات التي لا تملك برمجيات وكيل خاصة بها، وتُسمى هذه المرسلات مخدّمات الكفيل العمومية. وقد قامت شركة TIS بكتابة مجموعة برمجيات تدعى plug-gw تسمح للجدار الناري في طبقة التطبيق بمعالجة أي

بروتوكول يمر عبره دون الحاجة إلى برمجيات وكيل خاصة بهذا البروتوكول. ولا تمتلك هذه البرمجيات الدقة العالية في عمليات التحكم مقارنةً بمخدّمات الوكيل المتخصصة، لأنها لا تمتلك معلومات كافية لتحديد تصرف البروتوكول عند مروره من خلال الجدار الناري. وتعتبر برمجيات plug-gw حلاً وسيطاً ما بين الجدار الناري في طبقة الشبكة والمخدّمات الوكيلة.

Socks

وهي مرسلات تطبيق عمومية تُستخدم عادة للسماح بالنفاذ إلى خارج الإنترانت، وتسمح الـ Socks بالاتصال عبر البروتوكول IP بالحواسيب الممنوع الاتصال بها عبر جدار ناري. حيث أنها تقبل أساساً الاتصالات الخارجية المطلوبة من قبل المستخدمين الداخليين في الإنترانت، وتقوم بربطهم بمواقع الإنترنت الخارجية، ومن ثم تقوم بربط المعطيات ذهاباً وإياباً بعد انتهاء عملية بناء الوصلة.

تأتي هذه الـ Socks كنص برمجيٍّ ويجب ترجمتها من أجل كل مخدّم على حدة، والترجمة بسيطة نوعاً ما ولا تستغرق فترة زمنية طويلة ويمكن أن الحصول عليها من الموقع:

ftp.nec.com/pub/security/socks.cstc

ويمكن أن تعمل الـ Socks على Linux, SCO, AIX, Solaris, SunPS.

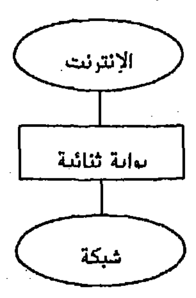
4-7-3 أشكال الجدار الناري

يمكن بناء الجدار الناري في شبكة الإنترانت بطرق مختلفة تعتمد على قرارات إدارة الشبكة في الموازنة ما بين الكلفة وأداء النظام الأمني المطلوب. وتستخدم معظم أنظمة الحماية المبنية على الجدار الناري تشكيلات (Configurations) متراكبة من عدة طبقات للحصول على أكبر درجات الحماية.

تُستخدم حالياً ثلاثة أشكال أساسية للجدار الناري يستخدم كلٌّ منها خصائص مختلفة، وهذه الأشكال هي:

1- البوابات ثنائية المقرّ

البوابات ثنائية المقرّ (Dual-homed gateways) هي حواسيب مضيفة معدّة لدعم واجهتي شبكة: إحدى الواجهتين موجهة إلى شبكة محمية داخلية، والأخرى موجهة خارجاً إلى شبكة خارجية. وهذه المضيفات ليست مهيأة لتوجيه حركة النقل بين الشبكتين، (الشكل 4-7).



الشكل (4-7): البوابات ثنائية المقرّ

تدعى البوابة ثنائية المقرّ أيضاً بالبرج المضيف (Bastion Host)، ومن المفترض أن تكون محميةً قدر الإمكان لأنها تشكّل الطريق الوحيد الذي يمكن أن يسلكه المخترق للوصول إلى موارد الشبكة الداخلية عن طريق الإنترنت. والبرج المضيف هو الحاسوب الذي يعمل عليه مخدّم الوب الخارجي ومخدّم FTP في الحالة الطبيعية، إضافةً إلى أنه يمكن أن يعمل كمخدّم بريد في الإنترنت، كما أنه الحاسوب الملائم لتشغيل مخدّمات الوكيل للمستخدمين الداخليين لتمكينهم من النفاذ إلى الإنترنت.

وأخيراً، تُعتبر البوابات ثنائية المقر النوع الأقل تكلفة من بين الأنواع الثلاثة المعروضة، ولكنها بالمقابل تعاني من نقطة ضعف لا يستهان بها، وتتمثل بأنه إذا سمحت أي برمجية تعمل عليها للمخترق بالولوج فإن كل الشبكة ستكون معرضة للاختراق عندئذ.

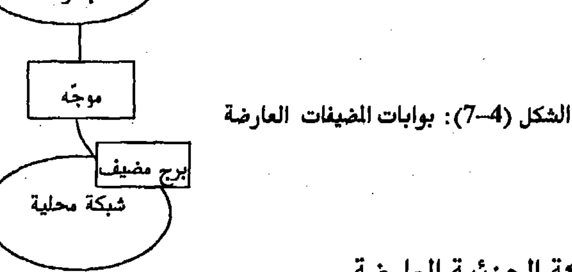
2- بوابات المضيفات العارضة

تُبنى بوابات المضيفات العارضة (Screened-host gateways) باستخدام موجّه عارض يقوم بإيقاف حركة نقل المعطيات إلى الشبكة الداخلية ويسمح بحركة النقل إلى البرج المضيف. وتملك هذه البوابات واجهة شبكة واحدة فقط، في حين تكون للبرج المضيف واجهتان كما ذكرنا آنفاً (الشكل 4-8).

تمتاز هذه البوابات بالنقاط التالية:

- على اعتبار أن معظم مزودي خدمة الإنترنت يضعون موجّهاً للموقع، فإن استخدام البنية السابقة يعتبر اقتصادياً وسهلاً.
- استخدام المضيفات العارضة يمكّن الشبكة من السماح لتطبيقات محددة بالنفاذ السهل إلى الشبكة الداخلية.

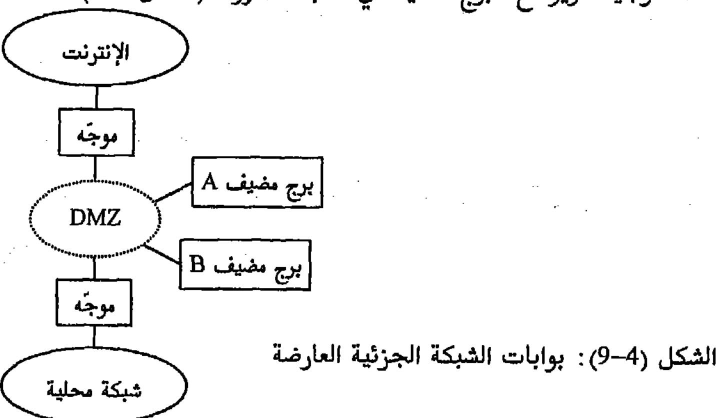
وتعاني هذه البوابات من نقطة ضعف، وهي أنها تعتمد على نظامي حماية منفصلين يجب أن يعملا على نحوٍ متكامل: الموجّه والبرج المضيف، وفي حال فشل أحدهما فإن الشبكة الداخلية ستصبح معرضة للاختراق.



الشكل (4-7): بوابات المضيفات العارضة

3- بوابات الشبكة الجزئية العارضة

تتألف بوابات الشبكة الجزئية العارضة (Screened-Subnet Gateways) من موجّهين عارضين يحيطان بالبرج المضيف ويحصرانه بينهما، فيصبح لدينا شبكة صغيرة معزولة ما بين القسم الآمن والشبكة الخارجية، ويوضع البرج المضيف في الشبكة المعزولة (الشكل 4-9).



الشكل (4-9): بوابات الشبكة الجزئية العارضة

من المكن وضع عدة مضيفات عارضة في الشبكة المعزولة (التي تُسمى المنطقة المنزوعة السلاح DeMilitarized Zone <DMZ>) لتحسين الأداء وزيادة الفعالية.

وهذه البنية هي البنية الأكثر كلفة من بين الأشكال الثلاثة المعروضة، ولكنها بالمقابل البنية الأكثر أمناً، حيث أن المخترق يحتاج إلى اختراق جهازي أمن معاً كي يتمكن من الوصول إلى الشبكة الداخلية.

4-8 الشبكات الافتراضية الآمنة الخاصة

قد تقوم أي شركة ببناء شبكة إنترانت لضمان الاستخدام الأمثل للموارد الحاسوبية التي تسمح باتصالات فعالة ضمن الشركة، كما تعطي للشركة واجهةً أفضل على العالم. ولكن كل هذه الميزات قد تكون غير كافية في العديد من الشركات التي يتطلب نشاطها أن تقوم بأعمال مباشرة مع شركاء عمل آخرين في مواقع مختلفة، أو مع الشركات الفرعية أو الشركات التي تقوم بشراء البضائع والخدمات، وغيرها.

يمكن لهذه الشركات تأمين الاتصال المباشر مع جميع العملاء الموجودين على شبكة الإنترنت على نحوٍ آمن باستخدام تكنولوجيا الشبكات الافتراضية الآمنة الخاصة (Virtual Saved Private Networks < VSPN>) التي تسمح لشبكتي إنترانت موصولتين إلى الإنترنت ببناء قناة اتصال افتراضية عبر شبكة الإنترنت، وتسمح هذه القناة بأن تتخاطب الشبكتان تخاطباً آمناً، وهذه الحماية للاتصال تتعلق بالطرق الخاصة المتبعة في هذا الوصل.

كما تُستخدم هذه التكنولوجيا لبناء إنترانت افتراضية في شركة ما تصل بين مكاتبها الفرعية على الإنترنت، وتضمن بالتأكيد أمن المعلومات المتبادلة عبر الإنترنت حيث لا يتمكن أحد من رؤيتها غير الأشخاص الموصولين في الإنترانت الافتراضية.

تقوم الشركات عند اعتماد تكنولوجيا VSPN بتوفير كميات كبيرة من الأموال كان يمكن أن تنفق كل شهر لاستئجار خطوط نقل معطيات خاصة لا يستخدمها أحد آخر وغير قابلة للاختراق، حيث أن شبكات VSPN توفر لهذه الشركات قنوات اتصال بنفس المواصفات المطلوبة من حيث الأمن، لكن مع إجراء كل حركة النقل عبر خطوط الإنترنت مما يسمح باتصالات إلكترونية أكثر فاعلية وذات مردود أكبر، حتى أنها قد تكون أكثر أمناً.

تستخدم التكنولوجيا VSPN مزيجاً من تكنولوجيا التوجيه وتكنولوجيا التشفير، إضافةً إلى تقنية تُسمى "حفر السراديب" (Tunneling)، حيث تقوم VSPN بتوجيه المعلومات المرسلة من إنترانت إلى إنترانت أخرى بطريقة مختلفة عن التوجيه المعتمد فيما لو كانت المعلومات مرسلة إلى موقع آخر غير آمن على الإنترنت. فهي تقوم بتشفير هذه المعلومات الأصلية (طرود IP) وتغلفها وترسلها عبر الإنترنت بعد التشفير لتظهر كمعلومات عادية (طرود IP عادية) يجري نشرها طبيعياً بواسطة الموجهات، ثم تقوم الإنترانت المستقبلة بفك تغليف هذه الطرود وفك تشفير المعلومات التي بداخلها، ومن ثم تنشر بواسطة الموجّهات الخاصة بتلك الإنترانت. وبالطبع لا أحد يستطيع قراءة المغلفات أثناء النقل عبر الإنترنت إلا إذا عرف طريقة فك التشفير اللازمة.

ويمكن تلخيص آلية عمل شبكات VSPN بالنقاط التالية:

- عندما ترغب إنترانت ما في إرسال معلومات خاصة إلى إنترانت أخرى بواسطة شبكات VSPN، فإنها لا تقوم بإرسال هذه المعطيات بطريقة تختلف عن تلك المتبعة عند إرسال معلومات عمومية لأي موقع على الإنترنت، فهذه المعلومات يجري أولاً تجزيئها إلى طرود TCP/IP.

- تتجه كل الطرود الخارجة من الإنترانت إلى مخدّم VSPN خاص، وهذا المخدّم يقوم بفحص كل الطرود IP ليرى فيما إذا كان الطرد متجه نحو إنترانت VSPN أخرى بدلاً من الإنترنت، ويجري ذلك بفحص عناوين IP في ترويسة الطرد وبفحص العنوان الهدف على ضوء قواعد المعطيات لعناوين VSPN، فإذا كان الطرد غير موافق لعناوين VSPN في قواعد

المعطيات فهذا يعني أن هذا الطرد موجه إلى الإنترنت العمومية، ولا يقوم المخدّم بأي عملية ويجري إرسال الطرد إلى وجهته كطرد عادي بواسطة الموجهات.

- إذا توافق عنوان IP للطرد مع عنوان VSPN تقوم برمجيات المخدّم بأخذ كامل محتوى الطرد TCP/IP (الترويسة والمعطيات) وتقوم بتشفيرها باستخدام تكنولوجيا تشفير فعالة لا يمكن فكها إلا باستخدام التكنولوجيا نفسها في الموقع الهدف.

- يجري وضع مغلف IP جديد حول الطرد المشفر، ويحوي هذا الغلف معلومات الطرد IP نفسها (عنوان المصدر والهدف، وغيرها) بحيث يبدو كطرد TCP/IP عادي يمكن أن ينشر عبر الإنترنت، ولكنه يكون غير قابل للقراءة من قبل أي أحد.

- يُرسل الطرد إلى الموجه الذي يقوم بنشره عبر الإنترنت على نحوٍ طبيعي ليجري التقاطه في الشبكة VSPN الهدف.

- يقوم مخدّم VSPN في الشبكة الهدف بفحص الطرود الواردة تباعاً، حيث يقوم بالتأكد من العنوان IP للمرسل فإذا لم يكن موافقاً للعناوين في قواعد المعطيات لشبكات إنترانت VSPN فإنه يرسل هذا الطرد ببساطة إلى موجّه إنترانت لينشره. أما إذا كان العنوان IP موافقاً، تقوم برمجيات المخدم بفصل المغلف IP وبفك تشفير الطرد TCP/IP للحصول على الطرد الأصلي.

- يُرسل الطرد أخيراً إلى موجه إنترانت ينشره نشراً طبيعياً إلى وجهته النهائية.

4-9 اختراقات شهيرة

سنقوم فيما يلي بعرض لبعض الاختراقات الشهيرة وكيفية تلافي حدوثها:

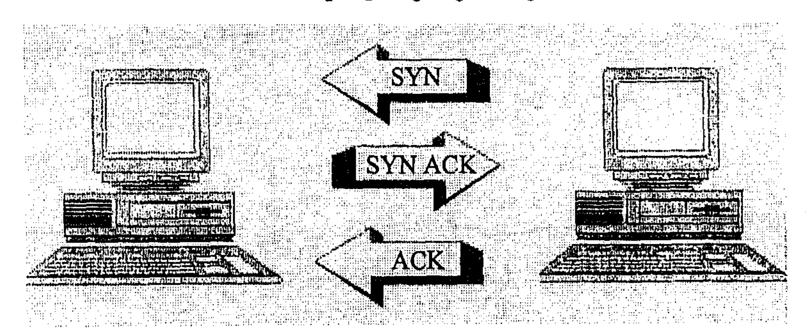
4-9-1 اختراق TCP SYN

المبدأ

عند البدء بجلسة TCP عادية يستقبل الحاسوب المستقبل طرداً يحمل الإشارة SYN في خانة المؤشرات في ترويسة رسالة TCP (راجع الفصل الثاني) من الحاسوب المرسل وذلك لطلب فتح وصلة TCP، فيستجيب الحاسوب المستقبل بإرسال الإشارة SYN ACK لإعلام الحاسوب المرسل بوصول رسالته لبدء جلسة الاتصال، ويجب على الحاسوب المرسل عندها أن يستجيب بإرسال إشارة ACK وهي رسالة إقرار باستلام الإشارة SYN ACK. بعد أن تجري هذه الخطوات الثلاث تكون وصلة TCP جاهزةً لتبادل المعلومات بين الحاسوبين، وتدعى العملية السابقة بمصافحة TCP الثلاثية.

في فترة الانتظار ما بين إرسال SYN ACK واستقبال إشارة ACK، فإن الحاسوب المستقبل يقوم بحجز جزء معين من الذاكرة لملاحقة الوصلة حتى تتم، وهذا الجزء من الذاكرة سيتحرر بسرعة لأن إشارة ACK متوقع وصولها بعد بضعة أجزاء من الثانية. ويمكن استغلال هذه الثغرة في تصميم البروتوكول TCP عند فتح الوصلة من خلال ما يُسمى بالاختراق TCP SYN، ويحدث هذا الاختراق عند إرسال طرود تحمل الإشارة SYN من الحاسوب المخترق بعناوين مصدر IP عشوائية، حيث يستجيب الحاسوب الضحية بإرسال SYN ACK رداً على كل منها، ويحجز جزءاً من الذاكرة منتظراً ورود الإشارة ACK. وبما أن الإشارات SYN ACK سوف تذهب إلى العناوين العشوائية فإن الرد لن يأتي أبداً، أي أن الجزء الأخير في المصافحة الثلاثية لن يجري، وتبقى الذاكرة المخصصة لكل طلب محجوزة لوقت معين، يكون في الغالب حوالي دقيقة، فإذا قام المخترق بإرسال الطرود SYN بالعناوين المزيفة وبمعدل إرسال سريع، فمن الممكن أن يزداد حجم الذاكرة المخصص لملاحقة

الوصلات عن الحد المسموح به مما يؤدي إلى امتناع الحاسوب الضحية عن تأدية الخدمة TCP، أو ما يُسمى TCP DoS (TCP Denial of Service)، ومن ثم فإن كل الخدمات والوظائف المعتمدة على هذه الخدمة مثل خدمة البريد الإلكتروني ونقل الملفات والوب ستتضرر، ولن تكون ملاحقة أثر المخترق سهلةً أبداً لأن عناوين المصدر IP تكون مزيفة وعشوائية.



الشكل (4-9): مصافحة TCP الثلاثية

الدفاع

تمكن معرفة حدوث هذا الاختراق عند ورود فائض من طرود SYN من عناوين مصدر عشـوائية، وأي جدار ناري مهيأ لصد الحجم اللامنتهي من طرود SYN هو جهاز محصّن ضد هـذا الاختراق، ولكن بالنسبة للحواسيب التي تقدم خدمات عامة (مخدّمات البريد الإلكتروني ومخدّمات الوب الموصولة على الإنترنت)، فإنه لا تمكن حمايتها بجدار ناري مهيأ كما سبق، لأن تهيئة هذا الجدار من أجل صد الحجم اللامنتهي من طرود SYN عشوائية يجري عن طريق تحديد مجموعة محدودة من عناوين IP مسموح لها النفاذ إلى المخدّم وهذا غير ممكن إذا أردنا تخديم الإنترنت، أي أنه لا يوجد دفاع أكيد ضد الاختراقات القادمة من عناوين عشوائية، ولكن هناك بعض الخيارات المتاحة والتي قد تخفف من تأثير هذا الاختراق:

- زيادة حجم الذاكرة المخصص لتتبع الوصلات.
- إنقاص زمن الانتظار اللازم لانتهاء مصافحة TCP الثلاثية.

- استخدام برمجيات خاصة لاكتشاف الشكلة والتحايل عليها (في حال توفر مثل هذه البرمجيات)، وهذا متعلق بنوع المخدّم المستخدم، إذ يجب التحقق من أن الشركة المصنعة للمخدّم قد أنتجت هذا النوع من البرمجيات فعلاً.

ملاحظة

إن ترشيح عناوين IP في المخدّم طريقة غير فعّالة لأن المخترق قد يغير عناوين IP، وقد يكون العنوان المرسل هو نفس عنوان أحد المستخدمين النظاميين.

4-9-2 اختراق Smurfing

أطلق هذا الاسم على اختراق "Smurfing" بسبب اسم أول برنامج قام باستغلاله، وهذا الاختراق من أحدث الاختراقات التي تعمل في سويّة الشبكة، ويستند هذا الاختراق على بعض نقاط الضعف في البروتوكول ICMP، حيث يُرسل المخترق عدداً كبيراً من تعليمات "echo" في بروتوكول ICMP (يمكن استخدام تعليمة "ping" في نظام UNIX)، ويكون عنوان الهدف هو عنوان التعميم (Broadcast)، وعنوان المصدر هو عنوان الحاسب الضحية (عنوان مزوّر طبعاً)، فإذا كان الموجه الذي يتحكم بحركة النقل إلى الحواسيب السابقة يقبل تمرير عناوين التعميم فإن جميع الحواسيب التي تصل إليها تعليمة "echo" سوف ترد عليها بـ "echo reply" مما يؤدي إلى زيادة حركة النقل بما يتناسب مع عدد الحواسيب المجيبة، ويمكن أن تكون هناك مئات الحواسيب التي ستجيب على كل طرد ICMP. هناك نوعان من التجهيزات التي تتأثر بهذا الاختراق:

- التجهيزات الوسيطة التي تمرر رسائل ICMP إلى الحواسيب الهدف.
- الحاسوب الضحية.

4-9-3 إعادة التوجيه في بروتوكول ICMP أو قنابل إعادة التوجيه

في عملية إعادة التوجيه في بروتوكول ICMP يُطلب من النظام المستقبل أن يتجاوز بعض المعلومات الموجودة في جدول توجيهه، هذه العملية لها استخداماتها النظامية، إذ تُستخدم من قبل الموجّهات لإخبار الحواسيب على الشبكة بأنها تستعمل طريقاً غير أمثلي، أو أنه لم يعد موجوداً، وذلك عند توجيه المعلومات إلى هدف محدد. وعندها يرسل الموجّه الخاطئ طرد ICMP خاص بإعادة التوجيه وذلك للإعلام بالطريق الصحيح الواجب استعماله.

إذا استطاع أحدهم تزوير طرد ICMP الخاص بإعادة التوجيه، والتقط الحاسوب الهدف هذا الطرد يصبح بالإمكان تعديل جدول التوجيه في ذلك الحاسوب، مما يؤدي إلى تدمير الحماية الأمنية للحاسوب وذلك عن طريق جعل حركة النقل تسلك طريقاً لم يخطط له مدير الشبكة.

كما يمكن توظيف إعادة التوجيه في بروتوكول ICMP في الاختراقات التي تؤدي إلى الامتناع عن التخديم، إذ يمكن إرسال طرد ICMP إلى حاسوب معين بحيث يفقد هذا الحاسوب الاتصال مع الشبكة أو بحيث لا يستطيع الوصول إلى شبكة معينة.

للدفاع ضد هذا النوع من الاختراقات يجب استعراض حركة النقل في الشبكة من خلال تشكيلة معينة من تشكيلات الجدار الناري، وذلك للحد من قدرة المخترقين على تنفيذ تعليمة "Ping" أو للحد من قدرتهم على تعديل جداول التوجيه.

الفصل الخامس

الخدمات الأساسية في شبكات الإنترانت

لقد عرضنا الخدمات الأساسية لشبكة الإنترنت بالتفصيل في كتاب آخر من هذه السلسلة. في هذه الفصل سنتعرض للخدمات نفسها باختصار آخذين بعين الاعتبار خصوصية الإنترانت (مقارنةً مع عمومية الإنترنت) كشبكة خاصة بمؤسسة ما.

5-1 الوب

5-1-1 إمكانيات موقع الوب على الإنترنت

إن استخدام تقنية الوب في شبكات الإنترانت يأتي كنتيجة طبيعية للعديد من الأسباب:

1- تسمح تقنية الوب بالتطوير عبر مختلف البنى المادية والبرمجية، حيث أن الصفحات المنهلة (HTML Pages) تظهر بالشكل نفسه على مختلف الأنظمة والبنى المادية، بحيث يصبح التركيز منصبّاً على تطوير التقنيات الجديدة بدلاً من معالجة مشاكل توافق البرمجيات.

2- إن شبكات الوب تعتمد على مفهوم زبون/مخدّم، وتسمح بتوظيف هذا المفهوم بسهولة.

3- تقنيات الوب منخفضة التكلفة بسبب التنافس الشديد في تسويق برمجيات المستعرضات (Browsers) ومخدّمات الوب (Web Servers)، وبما أنها تخضع للمعايير العالمية فهناك وفرة في البرمجيات المجانية.

4- تقنية الوب قابلة للتوسيع على نحوٍ جيد، حيث يمكن البدء بمخدّم للوب على حاسوب واحد وعدد قليل من الصفحات المنهلة. ويمكن أن تنمو بسهولة ليصبح لدينا مئات المخدّمات وآلاف الصفحات المنهلة.

5- يمكن بناء مواقع الوب في الإنترانت على شبكة المؤسسة المحلية الموجودة مسبقاً، مما يزيد من استثمارية الشبكة المحلية، كما أنه من السهل تأمين حماية مواقع وب الإنترانت مقارنة مع المواقع الموجودة على الإنترنت.

كما يمكن تلخيص مقدرات وفوائد بناء مواقع الوب على الإنترانت الخاصة بشركة ما بالنقاط التالية:

1- أتمتة إجراءات العمل

تقدّم مواقع الوب على الإنترانت (كما هي الحال على الإنترنت) عدداً كبيراً من الإمكانيات المؤثرة في تطوير طريقة تنفيذ العمل في الشركة. على سبيل المثال، تستخدم شركات متعددة مواقع الوب على الإنترانت لأتمتة توزيع وإدارة المستندات الداخلية مثل مستندات سياسات الشركة وإجراءاتها، والمعلومات المالية و قوائم الهواتف والمراكز الوظيفية. فالتوزيع الإلكتروني للمعلومات يلغي أثر التكلفة العالية في تحديث وتوزيع وثائق المستندات كل مرة تعدّل فيها الوثائق.

2- إعادة استخدام تقنيات زبون/مخدّم

إن إعادة اعتماد تقنيات زبون/مخدّم على أساس الوب في الإنترانت يؤمن نفاذاً عاماً للمعلومات بدون الحاجة إلى تثبيت وإدارة برمجيات زبون متخصصة، فيصبح بإمكان المستخدمين النفاذ إلى المعلومات المرغوب فيها من خلال المستعرضات. وتعتمد العديد من الشركات على تقنيات زبون/مخدّم في إدارة

الموارد البشرية والحسابات وخدمات إدارة المبيعات والمعلومات التنفيذية على مواقعها في الإنترانت الخاصة بها. كما أنّ اعتماد تقنيات زبون/مخدّم على أساس الوب أقل كلفة من ناحية الصيانة والإشراف من تقنيات زبون/مخدّم التقليدية.

3- نشر المعلومات

يمكن نشر المعلومات الداخلية ضمن مواقع الإنترانت على العاملين أو على الشركاء في العمل (كالموردين أو المقاولين). كما يمكن استغلال هذه المواقع لعرض المعلومات بطريقة حديثة وجذّابة، بحيث يصبح العاملون أكثرَ ميلاً للوصول إلى هذه المعلومات، وكذلك الأمر بالنسبة للشركاء الذين سوف يقدّرون إبقاءهم على اطّلاع على معلومات الشركة.

4- نشر ثقافة تعاونية

إن تدفق المعلومات الهامة بحرية أكبر على مواقع الوب يؤدي إلى جعل العاملين أكثر انجذاباً ومشاركة وتفاعلاً، سواء ضمن القسم أو مجموعة العمل الواحدة أو بين الأقسام ومجموعات العمل الأخرى.

5- زيادة رضى العاملين ودخلهم العكسي

تمكن الاستفادة من مواقع الوب لإبقاء العاملين على اطّلاع ولحثهم على التعبير عن ردود أفعالهم إزاء الأمور التي تهمّهم، مما يؤدي إلى بناء علاقة أكثر قرباً معهم، وبسبب مزايا مواقع الوب فيمكن تحصيل ردود أفعال العاملين وشركاء العمل بسهولة والاستفادة من هذه المعلومات لتحسين الخدمات ولدعم أداء هؤلاء الناس الذين لا غنى عنهم لعمل المؤسسة.

5-1-2 البروتوكول HTTP

بروتوكول HTTP هو بروتوكول نقل النصوص الفائقة (HyperText Transfer Protocol) ؛ ويقع هذا البروتوكول ضمن الطبقة السابعة في نموذج ISO/OSI وهو البروتوكول المعتمد في شبكة الـوب العالميـة. يتصف بروتوكول HTTP بأنه لا متصل (Connectionless)، أي يمكنه القيام بالعديد من الاتصالات السريعة بدون ضرورة إبقاء بوابة الاتصال مفتوحة. وبما أن حركة النقل في شبكة الوب لا تتطلب أكثر من بضعة كيلو بايتات (ثمانيات) لكل صفحة (ومن ثم يجري الانتقال إلى مخدّم آخـر)، فـإن تصميـم البروتوكول بأن يكون لا متصلاً هو مثالي لهذه الحالة. والسيئة الوحيدة في البروتوكولات اللامتصلـة في التطبيقات التجارية تكمن في كونها لا تحتفظ بالحالة (Stateless)، وهـذا يعـني أنـه لا يمكـن تتبع المستخدمين من خلال موقع الوب، لأنه في كل مرة نطلب فيها صفحة جديدة من الموقـع فإننـا نفتـح وصلة جديدة، وهذه العملية تستلزم فتح وصلة TCP وإغلاقها من أجل كل طلب مما قد يسبب الكثير من الضغط على الموقع في حالة الطلب الشديد.

يسمح بروتوكول HTTP بنوعين من الاتصالات عند إرسال الصفحات إلى المستعرض واستقبال الطلبات منه، كما أن هذا البرتوكول مصمم للسماح بنوع من التفاوض بين المستعرض والمخدّم على الرغم من أن هذه الميزة غير مستخدمة حالياً، وهذا ما سنناقشه فيما يلي:

1- التعليمات

هناك العديد من التعليمات في بروتوكول HTTP نذكر منها:

GET

تُستخدم هذه التعليمة لطلب أي نوع من المعلومات من المخدّم، ويجري تحديـد المعلومـات مـن خـلال عنوانها، حيث أن لكل نـوع مـن المـوارد علـى المخـدّم عنوانـاً وحيـداً URL (Uniform Resource Locator)، فإذا كان العنوان يدل على إجرائية تولّد المعلومات فإن المعلومات المتولـدة هـي المعلومـات التي سترسل إلى الزبون إذا كان المخدّم معدّاً لتنفيذ الإجرائية.

HEAD

تُستخدم هذه التعليمة للحصول على ترويسات المستند المرسل. تعطي هذه الترويسات بعض المعلومات الأساسية حول المستند من دون إرسال كامل المستند، وهي مشابهة للتعليمة السابقة إلا أن المخدِّم لا يرسل إلا ترويسة المستند. وتستخدم هذه التعليمة أيضاً لفحص صحة الارتباطات التشعبية وقابلية النفاذ إليها، ولتحديد التعديلات الأخيرة على المستند.

POST

تُستخدم هذه التعليمة لإرسال المعلومات إلى المخدّم، من خلال الأشكال الضمنية (Forms) عادة.

PUT

تُستخدم هذه التعليمة لإرسال بعض الملفات لتثبيتها على المخدّم. وعلى الرغم من أن توصيف البروتوكول HTTP/1.1 لا يحدد تصرف المخدّم تماماً في هذه الحالة، إلاّ أن بعض الأدوات البرمجية مثل Netscape Composer تستخدم هذه التعليمة لتحميل الملفات وتثبيتها على المخدّم.

DELETE

تُستخدم هذه التعليمة لطلب حذف ملف معين على المخدّم، وفي بعض أنظمة UNIX لا تعمل هذه التعليمة إذا كان المخدّم غير مسموح له بحذف الملفات من النظام.

TRACE

تُستخدم هذه التعليمة لتصحيح وتعقب الأخطاء.

يمكن الحصول على التفاصيل الكاملة عن البروتوكول HTTP 1.0 من RFC 1945، وعن البروتوكول HTTP 1.1 من RFC 2068.

2- ترويسات المستند

هناك العديد من الترويسات التي يجب أن ترسل مع المستند والتي يستخدمها كل من المخدّم والمستعرض لتمرير المعلومات بينهما. ويسمح بعض المخدّمات بقراءة هذه الترويسات مما يمكّن من

الاستفادة من المعلومـات الـواردة فيـها لاتخـاذ بعـض القـرارات بالنسـبة لمصممـي الـوب، ومـن هـذه الترويسات:

ترويسات القبول

تُستخدم من قبل بعض المستعرضات لقبـول مجموعـة محـارف، وقبـول الـترميز، وقبـول اللغـة. كمـا تستخدم أحياناً لتعريف نمط MIME (سنتحدث عنه لاحقـاً)، وكذلـك لتحديـد مجموعـة المحـارف المستخدمة والترميز واللغة التي يستطيع المستعرض التعامل معها.

ترويسات السماحية

تُستخدم لإعلام المخدّم بنوع السماحية المستخدمة، وهناك نوع واحد مستخدم للسماحية.

ترويسات المحتوى

تُستخدم لترميز المحتوى، لغة المحتوى، طول المحتوى، نمط المحتوى ؛ وهي معلومات مفيدة لكي يعرف المستعرض نوع محتوى المستند القادم من المخدّم.

ترويسة التاريخ

تُرسل هذه الترويسة من المخدّم ليعرف المستعرض تاريخ استجابة المخدّم.

ترويسة انتهاء الصلاحية

تُستخدم لإعلام المستعرض إلى متى يجب عليـه الاحتفـاظ بالصفحـة في الذاكـرة قبـل اسـتقدامها مـرة أخرى.

ترويسة المضيف

تُستخدم لتعريف المضيف الذي يدل عليه العنوان.

ترويسات التعديلات

تتضمن معلوماتٍ مثل آخر مرة جرى فيها تعديل المستند.

ترويسة الموقع

تُستخدم لإخبار المستعرض بأن المستند قد جرى نقله.

ترويسة المرجع

تُرسل من المستعرض لإخبار المخدِّم باسم آخر مستند جرى الوصول إليه.

ترويسة المخدِّم

تعطي معلومات عن المخدِّم.

ترويسة الزبون

تُرسل من الزبون لإعطاء معلومات عن برنامج الزبون (المستعرض).

ترويسة التحقق من الهوية

تُرسل من المخدِّم لإعلام المستعرض بأن التحقق منِ الهوية مطلوب.

هذه الترويسات هي أكثر الترويسات استخداماً، وهناك العديد من الترويسات الأخرى التي يمكن الحصول عليها من المراجع السابقة.

3- التفاوض حول المضمون

يسمح البروتوكول HTTP بالتفاوض بين المخدِّم والمستعرض حول شكل الملف واللغة، إضافةً إلى أمور أخرى، وهذه الميزة من الميزات الهامة وغير المستخدمة في البروتوكول HTTP، وتعمل على النحو التالي: يقوم البرنامج الزبون بطلب صورة مثلاً ويرسل مع الطلب قائمة بالأنماط التي يستطيع

معالجتها، عندها ينظر المخدّم إلى القائمة ويختار النمط الأفضل ثم يرسل الصورة. ويمكن أن تسمح هذه الميزة بالاتفاق على اللغة المستخدمة أو نوع تعدد الوسائط المرسل ؛ وفي الوقت الحالي لا توجد مستعرضات تدعم هذه الميزة، حيث يستعاض عنها بكتابة برامج Scripts لمعرفة الميزات التي يجب أن يمتلكها مستعرض معين، مما يعقّد عملية تطوير المواقع بخلق إشكاليات يمكن حلها إذا وجد مستعرض يستطيع معالجة الميزة السابقة.

4- تخبئة الصفحات (Caching)

بما أن شبكة الوب يمكن أن تُستخدم على الإنترنت، فإنه من الممكن تحسين الفعالية عن طريق تخزين المستندات التي استقدمت حديثاً في مخابئ مؤقتة في ذاكرة المخدّم الوكيل (إن وُجد)، ويجب الحذر في تنفيذ هذه العملية لأن مستندات الوب في تغيُّر مستمر. كما يمكن استخدام هذه التقنية في الإنترانت للتخفيف من حمل الشبكة، فالعديد من الشبكات المحلية تُقسم إلى شبكات فرعية، وترتبط هذه الشبكات الفرعية بوصلات قد تكون بطيئة أو سريعة، واستخدام تقنية التخبئة يساعد على تخفيف حركة النقل عبر الوصلات البطيئة كما يؤدي إلى التخفيف من حركة النقل الكلية. وكما رأينا فإن ترويسات HTTP تحتوي على العديد من المعلومات الكافية لتحديد فيما إذا كان الملف المخزّن يمكن أن يستخدم ولغاية أي تاريخ.

تعمل تقنية التخبئة كما يلي: يطلب البرنامج الزبون الصفحة من الوكيل، وعندها يقوم الوكيل بالتحقق من وجود الصفحة في مخبأ الذاكرة ومن أن هذه الصفحة حديثة، عندها يقوم بإرسال الصفحة من الذاكرة مباشرة من دون طلبها من المخدّم الفعلي، أمّا إذا كانت الصفحة غير موجودة أو غير حديثة فإن الوكيل يطلب الصفحة من المخدّم ويخبئها في الذاكرة بعد إرسالها إلى البرنامج الزبون.

وهناك أيضاً ترويسة انتهاء مدة الصلاحية التي تُعلم المخدّمات التي تستخدم تقنية التخبئة بالمدة التي تكون فيها المستندات صالحة للاستخدام (أي حديثة) دون أن تكون هناك حاجة لاستقدامها من المخدّم الفعلي.

تفيد هذه التقنية في تخفيف عرض حزمة نقل المستندات الكثيرة الطلب، وتدعم بعض المستعرضات هذه التقنية إذ تخزّن المستندات في الذاكرة والقرص المحلي، ويكتفي البعض الآخر بالذاكرة وهناك مستعرضات لا تقوم بهذه التقنية أبداً.

5-1-3 لغة HTML

يمكن اعتبار لغة تأشير النصوص الفائقة HTML (HyperText Markup Language) لغةً جزئيةً (أو وريثاً شرعياً) من لغة SGML (Generalized Markup Language)، حيث تعرّف هذه اللغة شكل عرض المعلومات (قوائم، عناوين، ارتباطات). تسمح HTML للمستعرضات بعرض المستندات وفق الشكل المنطقي للمستند، ولكنها لا تسمح بظهور المستند وفق تنسيق دقيق وثابت بسبب اختلاف طريقة العرض على شاشات العرض المختلفة. إلاّ أن لغة HTML تسمح بوصف المستند كما أنها تعطي للمستعرض المرونة في عرض النص بشكله الأفضل على الشاشة، وإحدى سيئات HTML هو أن التنسيق ليس دقيقاً على النحو الذي يمكن أن تقدّمه لغات البرمجة مثل Visual Basic، أو معالجات النصوص مثل FrameMaker، ومعايير HTML الجديدة تعمل على معالجة هذا الأمر، حيث يمكن القيام بالكثير من الأمور باستخدام مؤشرات (أو حاصرات Tags) HTML 4.0 وبرامج العرض الخارجية الحالية.

وتسمح لغة HTML بالميزة الأهم وهي التعامل مع الارتباطات التشعبية في المستندات، وهي المنطقة الحساسة التي تظهر في المستعرض وتسمح بالانتقال إلى مستند آخر، وهذا المستند الآخر ليس بالضرورة مستنداً نصياً فقد يكون صورةً أو صوتاً أو فيديو.

5-1-4 مخدّمات الوب

مخدّمات الوب هي برامج تستطيع التعامل مع بروتوكول HTTP، حيث تُستخدم للإجابة على طلبات HTTP وتجيب بأجوبة HTTP، وعموماً فإن أي مخدّم وب قادر على تنفيذ أي عملية

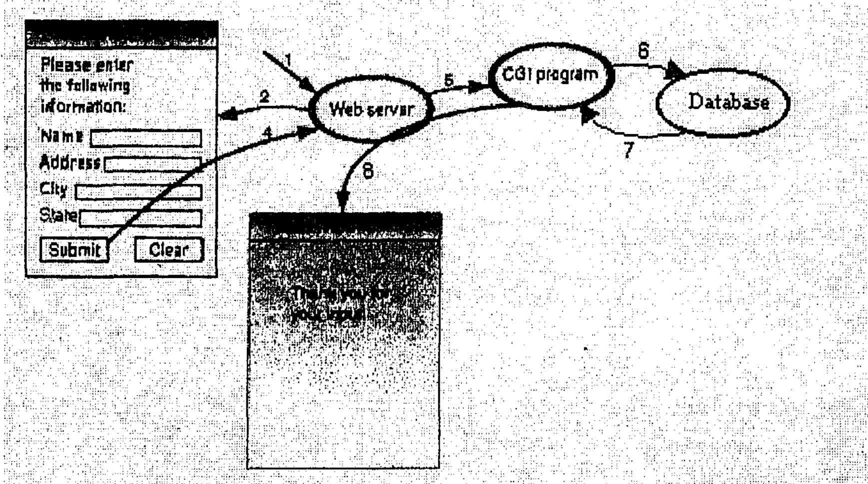
HTTP وإعادة المستندات والترويسات الصحيحة. وتمتلك المخدّمات الأكثر تعقيداً العديد من المزايا الإضافية التي تمكنها من تخديم مستندات HTML بسهولة أكبر، ومن أكثر الميزات شهرة التقنيات التي تسمح للمخدّم بتفسير الملفات أو تشغيل البرامج الخارجية، وتقنيات التحقق من الهوية الأكثر تعقيداً مثل استخدام ملفات (DBM) بدلاً من استخدام الملفات النصية، وميزات النفاذ المتقدّمة، وإدارة التحكم بالنفاذ اعتماداً على عنوان IP (تطرقنا لبعض هذه التقنيات في الفصل الرابع عند الحديث عن تحقيق الأمن بواسطة مخدّم الوب).

1- الملفات التفسيرية

لكي يتمكن المخدّم من تخديم صفحات منهلة ديناميكية لا بد من أن يمتلك القدرة على تفسير الملفات أو تنفيذ البرامج الخارجية، وهناك العديد من الطرق للقيام بهذا ولكن الطريقتين الأكثر شهرة هما SSI (Server Side Includes) أي إضافات المخدّم الجانبية، وتقنيات CGI (Common Gateway Interface).

- تسمح تقنيات SSI للصفحة المنهلة بأن تحتوي على معلومات ديناميكية تختلف باختلاف زمن طلب الصفحة، مما يسمح - مبدئياً - بتنفيذ بعض البرامج وإضافة الخرج إلى الصفحة المنهلة، وأحد الاستخدامات الشائعة لهذه التقنية توليد رأس وتذييل للصفحة المنهلة، بحيث يصبح بالإمكان تغيير مظهر الموقع ككل بتغيير ملف واحد أو ملفين، بدلاً من المرور على كافة الملفات المنهلة لتغييرها.

- تسمح تقنية CGI بتنفيذ برامج خارجية على المخدّم، ويمكن الاستفادة منها بكل شيء يمكن للبرنامج الخارجي أن يقوم به، والفرق الأساسي الوحيد بين برمجة CGI وأنواع البرمجة الأخرى هو في دخل البرنامج وخرجه. فدخل برامج CGI يأتي من وسائط (Parameters) يرسلها المستخدم إلى الزبون وفق شكل معياري ومن متحولات البيئة (Environment Variables) على المخدّم، وسنوضح هذه التقنية من خلال مثال لنموذج من التخاطب بين المخدّم والمستعرض للوصول إلى قاعدة معطيات على المخدّم باستخدام برنامج CGI.



الشكل (5-1): كيفية عمل CGI

يبين الشكل (5-1) نموذجاً لإدخال بعض المعلومات إلى قاعدة معطيات على مخدّم الوب، وتجري هذه العملية وفق الخطوات التالية:

1- يطلب المستخدم صفحة الإدخال عبر المستعرض الذي يتخاطب مع المخدّم لإرسال صفحة الوب التي تحتوي على نموذج (Form) الإدخال.

2- يرسل المخدّم الصفحة التي تحتوي على نموذج الإدخال.

3- يقوم المستخدم بتعبئة حقول هذه الصفحة.

4- عند الانتهاء يضغط المستخدم على زر Submit مما يؤدي إلى إرسال المعلومات المدخلة بواسطة البروتوكول HTTP، ويجري ذلك عادةً بإحدى الطريقتين GET أو POST (المذكورتين سابقاً).

5- عند وصول هذه المعلومات إلى المخدّم، يقوم هذا الأخير بدوره في تنفيذ برنامج CGI مع تزويده بالمعلومات المدخلة من المستخدم.

6- بما أن برنامج CGI يعمل على المخدّم فإنه يستطيع التخاطب مع قاعدة المعطيات لإدخال المعطيات المناسبة.

7- بعد إدخال المعلومات إلى قاعدة المعطيات ونجاح عملية الإدخال بدون أخطاء يستطيع برنامج CGI المتابعة.

8- يقوم برنامج CGI بتوليد صفحة الوب التي تُرسل كرد على طلب الزبون، وفي مثالنا نفترض أن عملية الإدخال تمت بدون أخطاء وأن الرد سيتضمن إعلام المستخدم بأن العملية قد تمت (من الممكن توليد أي رد مناسب في حالة ورود خطأ). بعد توليد هذه الصفحة يقوم برنامج CGI بتوجيهها إلى الخرج المعياري STDOUT، عندها يتلقى مخدّم الوب الخرج ويرسله للزبون بعد إضافة ترويسات HTTP المناسبة.

هناك العديد من التقنيات الحديثة التي تعمل على المخدّم لتوليد صفحات ديناميكية مثل تقنية ASP (Active Server Page) الخاصة ببيئة Windows وهي من التقنيات الفعّالة.

2- تسجيل الدخول إلى المخدّم

تحتاج العديد من المواقع لمعرفة من يستخدم مخدّم الوب وذلك لعدة أغراض كالإعلان عن دخول المستخدم أو للمساعدة في تحديد المزايا التي يرغب المستخدم في توفرها. ومهما كان السبب فإن تسجيل الدخول إلى المخدّم هو أحد أهم المزايا التي يمكن أن يمتلكها مخدّم الوب.

ويدعم العديد من مخدّمات الوب الحالية طريقة عامة للتسجيل تضم العديد من المعلومات مثل اسم حاسوب المستخدم، محدّد الاسم أو المجموعة، التاريخ والوقت، نوع طلب HTTP، حالة الطلب وعدد الثمانيات المرسلة. تقدّم مخدّمات الوكيل من Netscape أيضاً أشكالاً متقدّمة للملفات التسجيل وتضم تفاصيل أخرى عن العاملات مثل الاتصالات بين الوكيل والمخدّم وزمن النقل. تسمح مخدّمات Apache للمستخدمين بتحديد معلومات التسجيل لتسجيل المعلومات التي يريدونها من الترويسات.

3- واجهة الإدارة أو الإشراف

يمكن أن يصبح مخدّم الوب معقداً من حيث إدارته والإشراف عليه، وإحدى أهم صفات المخدّم هي سهولة إدارته. كانت هذه العملية - في المخدّمات الأولى - تجري عن طريق تحرير ملفات الإعداد مباشرة مما يتطلب معرفة معنى كل الخيارات المكنة وكيفية عملها بعضها مع بعض، وفي المخدّمات الحالية يمكن إدارة المخدّم عبر واجهة تخاطب بيانية مما يوفر على مدير الوب القيام بما قد يستلزمه إلى حل الإشكالات، كما أنها تجعل عملية تعديل الخيارات أسهل.

5-1-5 المستعرض

الوظيفة الأساسية للمستعرض هي النفاذ إلى الوب وعرض المعلومات المخزنة على المخدّمات البعيدة، حيث تكون هذه المعلومات مخزنة في الملفات المنهلة المكتوبة بلغة HTML، ومن ثم يقوم المستعرض بتحديد أفضل طريقة لعرض هذه المعلومات. تؤدي هذه العملية إلى المرونة في تحديد الطريقة الأنسب للنفاذ إلى المعلومات، وكما هي الحال بالنسبة للتقنيات التي أنتجت في القرن العشرين، فإن مصممي الوب لم يتخيلوا كل التطبيقات المحتملة لهذه التقنية، فعند ظهور الاستخدامات الجديدة للوب تغيرت المستعرضات لتحقيق الأهداف الجديدة لمستخدمي الوب.

1- أنماط MIME

تُستخدم هذه الأنماط لإعلام البرمجيات عن نمط المعطيات المخزنة في ملفٍ ما وهي اختصار لـ (Multipurpose Internet Mail Extension). فعند إرسال أي صفحة وب من المخدّم تكون هذه الصفحة مرفقة ببعض المعلومات بواسطة البروتوكول HTTP ومنها نمط MIME، حيث يقوم المستعرض بمقارنة نمط MIME القادم مع المستند من المخدّم مع قائمة من الأنماط المعرفة لديه مسبقاً لمعرفة كيفية عرض المستند. بعض الأنماط مثل text/html و text/plain يمكن أن يعرضها المستعرض بنفسه والبعض الآخر يحتاج إلى برامج خارجية، وسنناقش هذا الأمر لاحقاً. وقد يحتوي المستند

الواحد على أكثر من نمط، وكمثال على ذلك نذكر تضمُّنَ المستند لصور داخلية، فعندما يستقدم المستعرض المستند ويلاحظ وجود الصور الداخلية فإنه يطلبها من المخدِّم، فالصفحة التي تظهر في المستعرض تمثّل نمط MIME واحداً ولكن المستند ككل يتألف من عدة أنماط MIME. بعض المستعرضات مثل Netscape Navigator تطلب النص قبل الصور وبالتالي يمكن للمستخدم البدء بقراءة النص بدون انتظار استقدام الصور، وبعضها الآخر لا يطلب الصور أبداً مثل مستعرض Lynx، فهو مستعرض نصي فقط، وأغلب المستعرضات يقدم خيار استقدام الصور أو عدمه، وقد تُعرض الصور أثناء استقدامها، وهي تكون إما ملفات gif أو jpeg، وتبدأ بالظهور تدريجياً وتزداد وضوحاً حتى تكتمل معالمها مع انتهاء عملية الاستقدام، وفي حالات أخرى يقوم المستعرض بعرض الصورة من الأعلى إلى الأسفل، ومن الممكن أن يعرض المستعرض صور gif المتحركة، وهي تركيب من صور gif في ملف واحد بحيث تظهر الأجزاء بترتيب معين لتبدوَ الصورة وكأنها تتحرك.

وبالنسبة للأنماط التي لا يستطيع المستعرض عرضها فإنه يقوم بتنفيذ برنامج عرض خارجي، حيث ينظر في ملف خاص اسمه mailcap لمعرفة البرنامج المطلوب والوسائط التي يحتاجها هذا البرنامج، وقد تكون ملفات MIME وmialcap مخزنة في عدة أماكن، وذلك حسب المستعرض، وهناك مستعرضات تسمح بتحرير هذه الملفات من ضمن المستعرض نفسه، ويمكن معرفة ذلك من خلال ملفات المساعدة التي تأتي مع برنامج المستعرض.

ويكون ملف MIME عادةً على شكل مجموعة من الأسطر، وقد يكون شكل السطر:

```
mime-type     ext1, ext2
```

أما ملف mailcap فقد يحتوي على أسطر مشابهة للسطر التالي:

```
mime-type;    program [args]
```

والمقطع الخاص بالوسائط قد يحتوي على %s وتعني اسم الملف الحالي الذي يعلم المستعرض على استقدامه، فإذا أردنا مثلاً تنفيذ برنامج docview لعرض الملفات ذات النمط application/doc فيجب أن نضيف السطر التالي إلى ملف mailcap:

```
application/doc;      docview      %s
```

وإذا أردنا إضافة وسائط معينة لهذا البرنامج كخيارات العرض مثلاً فإننا نضيف السطر السابق مع التعديل:

application/doc; docview -view %s

تجدر الإشارة إلى أن استخدام ملفات MIME وmailcap في شبكات الإنترانت يسهل تخزين ملفات الشركة الخاصة والحصول عليها من مصدر مركزي، فإذا كانت الشركة تستخدم ملفات من نمط خاص وتعرض باستخدام تطبيق خاص، فبإضافة السطر المناسب إلى ملف MIME على كل من المخدّم وبرنامج الزبون، وكذلك الأمر بالنسبة للملف mailcap عند الزبون، يستطيع البرنامج الزبون تنفيذ التطبيق الخاص عندما يفعّل المستخدم أحد ملفات الشركة الخاصة.

ملاحظة

يمكن أيضاً إعداد ملفات MIME وmailcap لتنفيذ أي برنامج لتفسير الأوامر تلقائياً، مثل command.com أو /bin/sh، وعلى الرغم من أن هذه الطريقة تسمح بسهولة التعديل في البرمجيات ولكنها تفتح العديد من الثغرات الأمنية، لأن أي ملف يحمل نمط MIME الموافق سيجري تفسيره سواء أكان ملفاً موثوقاً أو ملفاً معداً من قبل بعض المخترقين على الإنترنت.

2- برامج العرض الخارجية

هي برامج عرض خارجية يعرف المستعرض كيفية استخدامها، حيث يقوم المستعرض بحفظ الملف في منطقة مؤقتة، ويستدعي برنامج العرض الخارجي ليقوم هذا الأخير بعرضه في نافذة مستقلة عن المستعرض، وقد يكون شكل هذه النافذة مختلفاً عن مظهر نافذة المستعرض، وهناك العديد من برامج العرض الخارجي وسنذكر أكثر هذه البرامج شهرة في عرض الأنماط التالية:

- *مستندات FrameMaker:* يمكن استعمال البرنامج FrameViewer من شركة Adobe المتوفر مجاناً (عنوان شركة Adobe هو http//www.adobe.com)، وهذا البرنامج متوفر في بيئة UNIX وبيئة Windows.

- *مستندات Adobe Acrobat:* تنتـج شـركة Adobe أيضـاً برنامجـاً مجانيـاً لعـرض وطباعـة ملفات PDF (Portable Document Format)، حيث تستخدم هذه الملفـات بـهدف عـرض الملفات وفق شكل محدد وثابت مهما كان نوع جهاز المستخدم.
- *مستندات Microsoft Word:* أنتجت شركة Microsoft برنامج عرض وطباعة لهذه الملفات وهو مجاني، ولكن لا يوجد برنامج موافق للعرض ضمن بيئة UNIX.
- *الصور البيانية:* يسمح برنامج LView بعرض العديد من أنماط الصـور البيانيـة وهـو برنـامج Shareware متوفر علـى العنـوان ftp://oak.okland.edu/SimTel، وهـو يعمـل ضمـن بيئـة Windows، وهنـاك البرنـامج XV علـى بيئـة UNIX ويمكـن الحصـول عليـه مـن العنـوان ftp://ftp.cis.upenn.edu/pub/xv.
- *الصوت:* أضافت Microsoft برامج لتشغيل الصوت ابتداءً من نظام التشغيل Windows 3.1 وهذه البرامج تتطلب بـالطبع وجـود كـرت صـوت، وبعـض حواسـيب UNIX تملـك برامـج للصوت مبيّتة داخلياً.
- *Mpeg Video:* تملك Microsoft برنامج Amovie على نظـام Windows 95 التوفـر علـى صفحـة Microsoft ويمـكن عـرض ملفـات الفيديـو مـن ضمـن برنـامج Media Player. أمّا بالنسبة لمستخدمي نظام UNIX، فيمكن الحصول على البرنامج mpeg-play من العنوان:

ftp://mm-ftp.cs.berkeley.edu/pub/mpeg/play.

تنفذ برامج العرض الخارجية في نافذة منفصلة، والمجموعة التالية من الـبرامج الـتي سـنقوم بعرضـها تُسمى Plug-ins، وهي برامج تضاف إلى المستعرض من شركات أخرى غير تلك التي أنتجت برنـامج المستعرض بهدف تمديد وظيفته.

Plug-ins -3

ابتداءً من مستعرض Navigator 2.0 أصبح بإمكان شركات البرمجيات أن تبني بسهولة أدوات إضافية لتعمل ضمن مستعرض Netscape، وهذه الأدوات تُبنى بهدف تمديد وظيفة مستعرض Netscape، وعلى النقيض من برامج العرض الخارجية فإنها تُدمج مع المستعرض وتبدو كجزء منه.

هذه الأدوات الإضافية المسماة Plug-ins تقوم بالعديد من المهام والتطبيقات المتعلقة بالصوت والرسم والتطبيقات ثلاثية الأبعاد، وهناك أيضاً أدوات تحويل النص إلى الصوت المتوفرة على بيئة الماكينتوش والمسماة Talker والتي تقرأ صفحة الوب للمستخدم.

4- اختيار المستعرض

بما أن المستعرض هو الجزء الأكثر استخداماً في الإنترانت فإنه الجزء الأكثر أهمية، وليس من السهل تغييره فيما بعد، ولذلك فإن اختيار المستعرض المناسب يجب أن يجري بكثير من الحذر والتخطيط المسبق، ومن المفضل استخدام مستعرض معياري على الإنترانت، لأنه إذا كان جميع المستخدمين يعملون على نفس الواجهة التخاطبية فإن عملية تطوير المستندات تصبح أكثر سهولة. فمصممو الصفحات يعرفون أي المزايا يجب استخدامها، وعادةً ما يجري تصميم الصفحات بما يتوافق مع أكثر من وسط مادي وبرمجي، مما يعني إما عدم إمكانية استخدام المزايا الحديثة في الصفحات المنهلة وإما كتابة صفحات منهلة تتوافق مع البنى الجديدة فقط. ومن الممكن التغلب على هذه المشكلة باستخدام بعض التقنيات مثل تقنية CGI، لكن هذا الحل سيؤدي إلى تكرار غير مرغوبٍ في كتابة صفحات لمعالجة جميع أنواع المستعرضات الممكن وجودها في الإنترانت.

والاعتماد على نوع واحد من المستعرضات يسهّل من تعامل المستخدمين أيضاً، حيث يصبح بالإمكان اختيار أي حاسوب واستعراض الصفحات من خلال واجهة مشتركة.

5-1-6 مثال: العلاقة بين المخدّم والمستعرض

لفهم كيفية عمل المخدّم والمستعرض عندما يطلب المستعرض ملفاً نعرض المثال البسيط التالي:

- يرسل المستخدم طلباً للحصول على مستند، لنفرض أن العنوان المطلوب هو:
http://www.company.com

- يتصل المستعرض عبر البوابة الافتراضية للبروتوكول HTTP ذات الرقم 80، ويطلب المستند الجذر عن طريق إرسال التعليمة "Get /"، والتي تعني طلب المستند الجذري وغالباً ما يكون index.html.

- يرى المخدّم الطلب نظراً لكونه يستمع إلى البوابة 80، ويبحث عن المستند الجذر، ويفحص المخدّم إعداداته لمعرفة ما هو الملف الجذر، وعادة ما يكون الإعداد باسم Document Root أو Directory Index.

- ثم يقوم المخدّم أيضاً بالتحقق من عدم وجود أي قيود للنفاذ إلى الملف، وإذا كان هناك أي قيد فإن المستعرض لن يحصل على الملف، ويعيد المخدّم رقم الخطأ.

- وإذا كان من المسموح النفاذ إلى الملف يولّد المخدّم ترويسة HTTP تتضمن على نمط MIME الملف (مثلاً "text/html")، ومن ثم يرسل المخدّم الترويسة والملف.

- يستقبل المستعرض الترويسة والملف ويفحص الترويسة لمعرفة كيفية عرض الملف، ومن ثم يعرض الملف. وإذا لم يستطع المستعرض عرض نمط MIME الملف فإنه يستدعي برنامج عرض خارجي أو أنه يقوم بحفظ الملف على القرص الصلب.

5-2 نقل الملفات

تُعتبر خدمة نقل الملفات بواسطة البروتوكول FTP من الخدمات الأساسية في الإنترنت والإنترانت، وهي من الخدمات المفيدة في التشارك على الملفات. كما أن الاستثمار الجيد لهذه الخدمة يساعد في تحرير حركة النقل على الشبكة.

سنناقش فيما يلي كيفية عمل هذه الخدمة وكيفية الاستخدام الأمثل لها، إضافةً إلى استعراض مختلف أنواع البرمجيات التي تحقق هذه الخدمة مع إبراز النقاط الإيجابية والسلبية في كل منها. ومن المهم أيضاً فهم الأمور المتعلقة بالدخول إلى مخدّم FTP، وكيفية التحقق من وثوقية طلب الدخول، فإذا كان هناك ما يجب التوقف عنده فهو هذا الأمر، لأن أي تهاون في عملية الإدخال قد يعرّض كامل الشبكة للخطر.

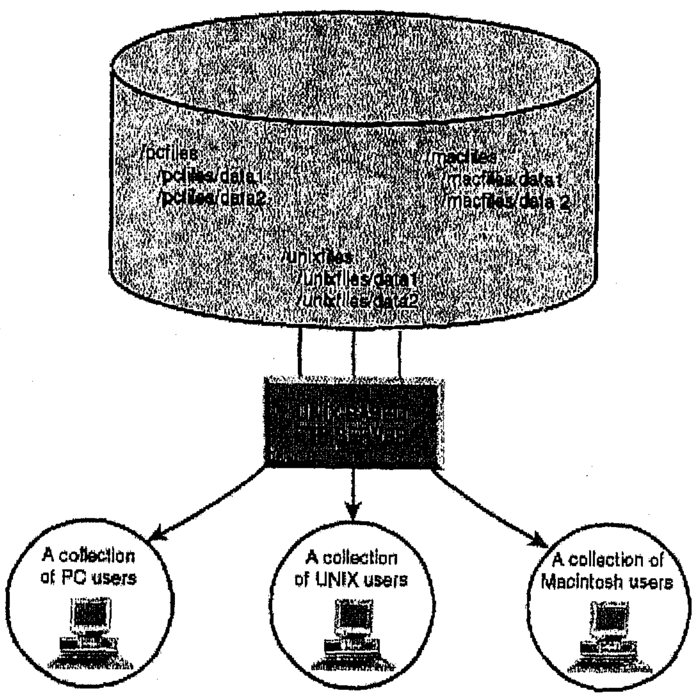
5-2-1 بروتوكول FTP

يعمل بروتوكول FTP ضمن طبقة التطبيقات في نموذج ISO/OSI، حيث تقع معظم تطبيقات TCP/IP التي تتفاعل مباشرة مع المستخدم، وكانت خدمة نقل الملفات من الأدوات الرئيسية المطلوبة في الشبكات طوال عقدين من الزمان، ولها تاريخ في معظم الأنظمة الرائدة.

وقد ساهم انتشار الإنترنت كأداة مساعدة للأعمال في انتشار خدمة نقل الملفات بعد أن كانت حكراً على العلماء والخبراء. وأصبحت هذه الخدمة اليوم من الخدمات الشعبية بين المستخدمين إذ أصبح من الممكن استخدامها من خلال لمستعرضات الوب والبرامج المماثلة.

من أهم أسباب استخدام بروتوكول نقل الملفات FTP في الإنترانت هو استقلاليته عن البنية المادية، فهو يسمح بنقل الملفات بين مختلف أنظمة التشغيل. وليس من الضروري أن تكون الملفات المخزنة على المخدّم متوافقة مع نظام تشغيل المخدّم إذ يمكن أن يكون المخدّم على نظام UNIX ويحتوي

ملفات تحوي برامج خاصة بأي نظام آخر مثل ماكينتوش أو Windows ، كما يتضح ذلـك في الشـكل (5–2).

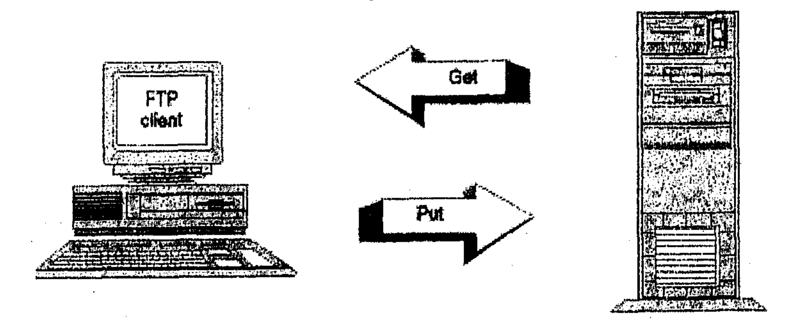


الشكل (5–2): استقلالية FTP عن البنية المادية

5–2–2 العلاقة بين الزبون والمخدّم

يعمل بروتوكول FTP بين نظامين: الأول هو الذي يطلـب نقـل الملفـات (الزبـون) والثـاني هـو الـذي يوافق على الطلب ويقوم بالاستقبال والإرسال (المخدّم). نظام الزبون هو عبـارة عـن واجهـة تخاطبيـة تجعل من بروتوكول FTP أكثر قابلية للاسـتخدام بالنسـبة للمسـتخدم النـهائي، حيـث تسـمح هـذه الواجهة للمستخدم بإدخال المعلومات اللازمة لجلسة نقل الملفات.

تتجلى نواة بروتوكـول FTP في التعليمتـين get وput، حيـث تقـوم الأولى بطلـب ملفـات مـن المخـدّم لتنقلها إلى المجلد الحالي عند المستخدم، أما التعليمة الثانية فتقوم بنقل الملفات بالاتجاه المعـاكس أي من المجلد الحالي في نظام المستخدم إلى المخدّم، ويوضّح الشكل (5-3) هذه العملية.



الشكل (5-3): الفرق بين تعليمتي get وput

لا يعمل نظام المخدّم مثل تطبيق الزبون، إذ يعمل تطبيق المخدّم في الخلفية، ويبقى غـير فعّـال إلى أن يتصل مستخدم ما به، عندها ينشط هذا المخدّم ويرسل إقراراً للمستخدم بوصول طلبه، ثم يقوم بمـهام التحقق من وثوقية الطلب، فيتحقق من اسم المستخدم وكلمة السر.

يظهر مخدّم FTP بأشكال مختلفة في أنظمة التشغيل، ولكنه لا يكـون برنامجـاً تنفيذيـاً، بـل إجـراءً على حاسوب معين يعمل كمخدّم، ويأخذ أشكالاً وأسماءً تختلف بحسب نظام التشغيل كما هو مبـين أدناه.

Platform	**Implementation of FTP Server**
UNIX	Daemon
MS-DOS	TSR that can be invoked as executable
Windows NT	Service
Mac	Extension

5-2-3 تعليمات FTP

فيما يلي قائمة بأوامر FTP التي يتعامل معها التطبيق ftp في بيئة Windows 95، (قد تكون هناك تعليمات إضافية في أنظمة أخرى):

!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	
close	lcd	open	rmdir	

الجدول (5-1): تعليمات FTP

سنستعرض فيما يلي الأوامر الأساسية المستخدمة في نقل الملفات:

1- بداية الجلسة

لبدء جلسة FTP يجب تنفيذ تطبيق الزبون وذلك بإحدى طريقتين، إما بكتابة اسم التعليمة مع اسم مخدّم نقل الملفات كما يلي: "ftp <server-name>"، وإما بكتابة التعليمة "ftp" فقط (انظر التعليمة open لمعرفة كيفية المتابعة)، ونلاحظ بدء تنفيذ العمل عند ظهور "ftp>" على الشاشة.

2- الحصول على المساعدة أثناء الجلسة

يمكن الحصول على المساعدة بكتابة "help" أو "?"، يقوم البرنامج عندئذٍ بعرض قائمة بكل التعليمات المتوفرة، كما هو موضح في الجدول (5-1)، وللحصول على المساعدة حول تعليمة معينة نكتب "help <command>" فيعرض البرنامج شرحاً مبسطاً لهذه التعليمة.

ASCII -3

نستخدم هذه التعليمة لتحويل نمط النقل إلى النمط النصي بدلاً من النمط الثنائي (انظر التعليمة binary)، هذا النمط من النقل خاص بالمعطيات النصية أو المعطيات ASCII وهو نمط فعّال وسريع، ويكون عادةً النمط الافتراضي لأن الملفات تنتقل بسرعة أكبر باستخدام هذا النمط، ولكن يجب الانتباه إلى أن البرامج التنفيذية المنقولة باستخدام هذا النمط لن تعمل بعد نقلها، وهذا الخطأ من الأخطاء الشائعة عند استخدام خدمة نقل الملفات، وكذلك لا يمكن نقل الصور أو أي نوع من الملفات غير النصية نقلاً صحيحاً باستخدام هذا النمط.

Binary -4

هذه التعليمة هي التعليمة المرافقة لتعليمة ASCII، حيث تحول نمط النقل إلى النمط الثنائي، مما يعني أن المعطيات ستنتقل ثُمانيةً ثُمانية، بينما تنتقل المعطيات في النمط السابق حرفاً حرفاً (حسب تمثيل الـ ASCII لهذه الأحرف). وعلى الرغم من أن هذا النمط من النقل يضمن نقل الملفات كاملة ودون أخطاء في النقل إلا أنها تأخذ زمناً أكبر من زمن النقل النصي، ولكنها الطريقة الوحيدة لنقل الملفات التنفيذية.

bye -5

تُنهي هذه التعليمة جلسة نقل الملفات كما تُنهي تنفيذ برنامج الزبون، وهي مطابقة لتعليمة "quit"، وقد أوجدت لتكون التعليمات مألوفة أكثر للمستخدمين الذين يتعاملون مع الـ Mainframes أكثر من تعاملهم مع الحواسيب الشخصية أو الماكينتوش.

cd -6

تسمح هذه التعليمة بالتنقل ضمن نظام ملفات المخدّم، وتعمل على نحوٍ مشابه لتعليمة "cd" في نظامي UNIX و DOS. مثلاً التعليمة ".. cd" تنقل المستخدم إلى مجلد أعلى، بينما تعني النقطة '.' المجلد

الحالي، ويمكن استخدام كل من الشرطة الأمامية والخلفية كفواصل بين أسماء المجلدات أي أن كلتا التعليمتين "cd /usr/bin" و "cd \usr\bin" صحيحتان.

close -7

تُنهي هذه التعليمة جلسة النقل مع المخدّم بدون أن تنهي البرنامج، وبالتالي تمكن معاودة الاتصال مع مخدّم آخر دون الحاجة إلى إعادة تشغيل البرنامج في كل مرة (انظر التعليمة "open").

dir -7

تعمل هذه التعليمة على نحوٍ مماثل لتعليمة "dir" في نظام DOS، حيث تسمح باستعراض محتويات مجلد العمل الحالي على نظام المخدّم.

get -8

تقوم هذه التعليمة بنقل الملف المحدّد من مجلد العمل الحالي في نظام المخدّم إلى مجلد العمل الحالي في نظام المستخدم، ولا تسمح هذه التعليمة بنقل أكثر من ملف في آن واحد، (انظر التعليمة "mget").

hash -9

من المفضل استخدام هذه التعليمة عند نقل الملفات الكبيرة، حيث أن تنفيذ هذه التعليمة يؤدي إلى طباعة المحرف '#' على شاشة المستخدم عند إتمام كل عملية نقل جزئية، وبالتالي عند نقل الملفات الضخمة فإن استمرار طباعة المحرف السابق على الشاشة يضمن للمستخدم أن النظام ما زال يستجيب ولم يتوقف عن العمل لسبب ما، ولإلغاء عملية الطباعة على الشاشة يجب تنفيذ هذه التعليمة مرة ثانية للتبديل بين النمطين: طباعة أو عدم طباعة.

lcd -10

تغيّر هذه التعليمة مجلد العمل الحالي على نظام المستخدم، وقواعد هذه التعليمة مطابقة لتعليمة "cd" وهي اختصار لكلمة "Local Change Directory"، وعند تنفيذها بدون وسائط فإنها تقوم بعرض مجلد العمل الحالي في نظام المستخدم.

ls -11

تقوم هذه التعليمة بعرض محتويات مجلد العمل الحالي على نظام المخدّم، وهي مطابقة تماماً لتعليمة "dir"، والهدف منها هو أن تكون أوامر نقل الملفات مألوفة لمستخدمي كل من الحواسيب الشخصية وأنظمة UNIX.

mget -12

تقوم هذه التعليمة بوظيفة النقل كتعليمة "get"، ولكنها تسمح بنقل مجموعات من الملفات كما يوحي اسمها (multiple get) من نظام المخدّم إلى مجلد العمل الحالي على نظام المستخدم. وتفسر هذه التعليمة المحرف '*' كحرف خاص يعني أي سلسلة من الحروف، وتطلب من المستخدم الإجابة بنعم "Y" أو لا "N" من أجل كل ملف. مثلاً تنفيذ التعليمة "* mget" يؤدي إلى نقل جميع الملفات في مجلد العمل الحالي على نظام المخدّم بعد سؤال المستخدم عن كل ملف، ولا تستطيع هذه التعليمة نقل المجلدات والمجلدات الفرعية فيها تكرارياً. كما أنه لا يمكن إلغاء عملية سؤال المستخدم عن كل ملف، ولذلك فإن برامج نقل الملفات ذات الواجهة التخاطبية البيانية تقدم أسلوباً أكثر سهولة عند نقل العديد من الملفات. وفي بعض الحالات قد تكون التطبيقات التي تستخدم الأوامر النصية أفضل، وذلك يعتمد على قوة الواجهة التخاطبية التي توفرها التطبيقات ذات الواجهة التخاطبية البيانية.

mput -13

تعمل هذه التعليمة مثل التعليمة السابقة في نقل العديد من الملفات، ولكنها تقوم بالنقل من نظام المستخدم نحو نظام المخدّم، وكما في حالة "mget" فإن هذه التعليمة لا تستطيع نقل المجلدات والمجلدات الفرعية بصورة تكرارية.

open -14

تقوم هذه التعليمة بفتح جلسة اتصال جديدة مع مخدّم FTP، على أن تكون الجلسة السابقة قد انتهت (أي أن نكون قد نفذّنا التعليمة "close" لإنهاء الجلسة).

put -15

هذه التعليمة هي المرافقة لتعليمة "get" إذ تقوم بوظيفة النقل نفسها ولكن بالاتجاه المعاكس، أي أنها تنقل الملف المحدد من مجلد العمل الحالي على نظام المستخدم إلى مجلد العمل الحالي في نظام المخدّم.

pwd -16

تقوم هذه العملية بطباعة اسم مجلد العمل الحالي على نظام المخدّم.

quit -17

تنهي هذه التعليمة تنفيذ البرنامج ككل بعد إنهاء أي الجلسة الحالية، وهي مطابقة لتعليمة "bye"، والهدف من وجودها هو أيضاً أن تكون أوامر نقل الملفات أكثر تآلفاً مع المستخدمين.

User -18

تسمح هذه التعليمة بتغيير اسم المستخدم في أي جلسة اتصال مفتوحة مع المخدّم، وبعد إرسال اسم المستخدم الجديد يطلب المخدّم كلمة السر وفي حال المطابقة تصبح جلسة الاتصال مفتوحة مع هذا المستخدم.

إن التعليمات التي قمنا بعرضها سابقاً هي التعليمات الأساسية اللازمة لنقل الملفات، ولكن يجب أن نذكر أن البروتوكول FTP يقدم تعليمات أخرى مثل تعليمات الحذف وتغيير أسماء الملفات على نظام المخدّم.

5-2-4 حساب FTP العام

عند طلب استقدام (Downloading) أي ملف من صفحة وب معينة يجري النقل باستخدام بروتوكول نقل الملفات FTP، وكنا قد ذكرنا أن الدخول إلى مخدّم FTP يتطلب حساباً على ذلك المخدّم وكلمة سر مرفقة به. لكن في الحالة السابقة وفي حالات مشابهة أخرى يجب أن نسمح لأي مستخدم باستقدام بعض الملفات باستخدام بروتوكول نقل الملفات FTP، ولذلك فإن بروتوكول FTP يقدم خدمة نقل الملفات لأي شخص كان من خلال حساب مخصص لهذه الغاية يُسمى Anonymous FTP، وسنسميه فيما يأتي الحساب العام.

خصوصية الحساب العام

في الفقرة السابقة قمنا باستعراض أهم تعليمات FTP الخاصة بنقل الملفات، وهناك العديد من التعليمات الأخرى التي لم نناقشها مثل تعليمات delete و mkdir و rename، التي يمكن أن تؤثر على بنية الملفات في نظام المخدّم. فإذا أردنا تقديم خدمة نقل الملفات من خلال الحساب العام إلى كل المستخدمين، فيجب ألا نقدم هذا المستوى من الحرية في التعامل مع ملفات نظام المخدّم، ولهذا السبب فمن غير الممكن حل مشكلة ضرورة وجود حساب خاص بكل المستخدمين بتخصيص حساب باسم وكلمة سر عامين (مثل guest). ولذلك أوجد الحساب العام لحل هذه المشكلة وذلك بتقديم خدمة نقل الملفات لكل المستخدمين ولكن مع السماح بتنفيذ مجموعة محددة من التعليمات حصراً، كما يسمح أيضاً برؤية جزء محدد من نظام ملفات المخدّم، فمثلاً يستحيل تنفيذ تعليمة "cd \" للانتقال إلى أعلى البنية الشجرية في نظام ملفات المخدّم باستخدام الحساب العام.

وعندما يُهيأ الحساب العام تهيئةً جيدةً، يصبح بإمكان أي شخص أن ينقل الملفات من نظام المخدّم بكتابة (Anonymous) عند طلب اسم المستخدم، وعلى الرغم من أن طلب كلمة السر سيتبع هذه العملية إلى أن كتابة أي كلمة أو عدم كتابة شيء سيسمح للمستخدم بالنفاذ إلى المخدّم، ومن آداب الإنترنت أن يكتب المستخدم عنوان بريده الإلكتروني وبذلك يستطيع مدير النظام معرفة من يزور المخدّم، وبكل الأحوال فإن المستخدم مسموح له بالنفاذ إلى جزء محدد من نظام ملفات المخدّم.

إعداد الحساب العام

لشرح عملية إعداد الحساب العام سنعرض مثالاً عن إعداد حساب عام في مخدّم FTP يعمل ضمن نظام UNIX، وهذا يتطلب من القارئ معرفة مسبقة بهذا النظام وإلا فيمكنه تجاوز هذه الفقرة. أمّا بالنسبة للحواسيب الشخصية وحواسيب ماكينتوش فيجري الإعداد من خلال واجهة تخاطبية تتألف من عدد من صناديق الحوار وليس من خلال الأوامر النصية.

1- بناء حساب عام في نظام UNIX

في البداية يجب بناء حساب باسم ftp ضمن مجموعة باسم anonymous، وذلك بأن نضيف إلى الملف /etc/group سطراً باسم المجموعة الجديدة anonymous، ويجب التأكد من أن محدد هذه المجموعة وحيد (Group ID) وغير مستخدم من قبل أي حساب آخر على النظام، من ثم تجب إضافة اسم المستخدم ftp إلى الملف /etc/passwd، وكذلك يجب أن يكون له محددٌ وحيدٌ (User ID) كما يجب أن يكون عضواً في المجموعة الجديدة. أمّا بالنسبة لحقل كلمة السر الخاصة بهذا الحساب فيجب أن يحتوي على المحرف "*" (بدون علامات التنصيص). ويمكن أن نكتب في الحقل الخاص بلغة الأوامر (Shell) النص: /bin/false، وذلك كاحتياط أمني يهدف إلى زيادة صعوبة عملية الدخول إلى هذا الحساب أو اختراقه. مثلاً إذا حجزنا الرقم 50 كمحدد للمستخدم والرقم 60 كمحدد للمجموعة فإن الملفين السابقين يجب أن يحتويا على الأسطر التالية:

/etc/group:

anonymous:*:60

/etc/passwd:

ftp:*:60:50::home/ftp:bin/false

نلاحظ أن مجلد الوطن (Home directory) لهذا الحساب هو home/ftp، ويجب اختيار هذا المجلد بحذر شديد، لأن هذا المجلد ومحتوياته ستكون مرئية من خلال الحساب العام. فعندما يدخل أي مستخدم إلى هذا الحساب يُنفّذ النظام إجراءً يُسمى chroot. يغيّر هذا الإجراء المجلد الجذري لنظام الملفات إلى المجلد الذكور في الملف /etc/passwd، ومن ثم فإن تعليمة "cd \" ستنقل المستخدم إلى هذا المجلد وليس إلى أعلى مستوى.

2- بناء مجلد الوطن

بما أن جميع الملفات والمجلدات التي تقع فوق المجلد الذي حُدّد كمجلد موطن للحساب العام غير متاحة للمستخدم، فلا يمكن الوصول إلى بعض التعليمات مثل تعليمة "ls" الخاصة باستعراض المجلدات في بيئة UNIX، والتي يستخدمها برنامج FTP الزبون عند طلب تنفيذ تعليمة "dir" أو "ls"، علماً أن هذه التعليمات ضرورية لعمل برنامج الزبون. لذلك يجب وضع نسخة من هذه التعليمة ومن التعليمات الأخرى الضرورية ضمن مجلد الوطن، ليصبح بالإمكان استعمالها مع محاولة تقليل عدد هذه التعليمات قدر الإمكان، والاستغناء عن وضع التعليمات والأدوات التي قد تسبب حدوث اختراق في النظام. لكن يجب نسخ التعليمة /bin/ls على الأقل إلى مجلد فرعي ضمن مجلد الوطن، وبالطبع يجب أن نعطي ملفات هذه التعليمات سماحية التنفيذ فقط لمنع أي محاولة لتغييرها أو قراءتها (بجعل السماحية 111 مثلاً باستخدام التعليمة "chmod").

وإذا أردنا السماح لتعليمة "ls" بعرض معلومات تفصيلية عن المستخدمين الذين يملكون الملفات في مجلد الوطن، فيجب وضع نسخة من الملفات /etc/group و /etc/passwd ضمن مجلد الوطن، ومن ثم يصبح بإمكان النظام مطابقة محدد المستخدم ومحدد المجموعة مع المعلومات الموجودة في هذه الملفات وعرضها من خلال تعليمة "ls -l"، وطبعاً يجب وضع المحرف "*" في حقل كلمة السر

(المشفّرة) في ملف /etc/passwd لاعتبارات أمنية، ولتأمين حماية أكبر يمكن حذف جميع الأسطر ماعدا الأسطر الخاصة بالمجموعات root، daemon، uccp، ftp، بحيث لا يمكن الحصول على أي اسم من أسماء المستخدمين المتواجدين على نظام المخدّم، وبالتالي يجب أن تكون سماحية هذه الملفات 444. وإذا أردنا السماح لمستخدمي الحساب العام بوضع ملفات ضمن مجلد الوطن فيجب أن نبني مجلداً جديداً يكون عادةً باسم pub ونسمح بالكتابة فيه، أي يجب أن تكون سماحيته 755. في النهاية يجب اختبار الحساب العام جيداً والتأكد من عدم وجود ثغرات في تهيئته يمكن أن تستغل لاختراق النظام.

5-2-5 مخدّمات نقل الملفات

يُعتبر اختيار المخدّم أهمّ من اختيار برنامج الزبون لأن مخدّم FTP يتعامل مع الأمن، وفي هذه الفقرة سنعرض الاختلافات بين مخدّمات FTP على مختلف أنظمة التشغيل، وكيف يتعامل كل منها مع الأمور المتعلقة بالأمن وحساب FTP العام.

UNIX/Linux -1

يأتي مع كل من هذين النظامين مخدّم FTP كجزء منهما باسم ftpd، وتحقيقه للحساب العام قوي، إضافةً إلى أنه موثق جيداً بالعديد من المراجع وصفحات الدليل (Manual <man>).

يمكن القول أن نظام UNIX هو أفضل نظام تشغيل يعمل عليه مخدّم نقل الملفات لأن هذه المخدّمات مرتبطة مباشرة بحسابات المستخدمين وكلمات السر، بحيث أن نظام التشغيل هو الذي يقوم بعملية إدارة الحسابات والتحقق من هوية المستخدم وكلمة السر. كما أن ميزة سماحيات الوصول إلى الملفات في هذا النظام تضيف مستوى آخر من الحماية لمخدّم FTP. وبالطبع فإن إحدى الإيجابيات الكثيرة لمخدّمات FTP على نظام UNIX، هي كون المخدّم جزءاً من النظام، أي أنه تطوّر مع تطور هذا النظام ومع تطور بناء الوظائف الحرجة في النظام طوال عقدين من الزمن.

2- MS-DOS/Windows 3.x/Windows 9x

إن مخدّم FTP في هذه الأنظمة لا يأتي كجزء من النظام، ولذلك فعند مقارنة المخدّمات المتوفرة تجب مراعاة كيفية تحققها من هوية المستخدم، وكذلك كيفية تعاملها مع الحساب العام، وعزل الأماكن العامة عن نظام الملفات. وبما أن نظام MS-DOS لا يسمح للمستخدم بالتحكم، فإن الحماية الأمنية المتوفرة في مخدّمات FTP على هذا النظام هي الحماية التي تحققها مجموعة TCP/IP البرمجية المستخدمة.

ولا يُنصح باستخدام هذا النظام لمخدّم FTP إذا كان الخيار الآخر هو نظام UNIX، لأنه يمكن إعداد الحاسوب الشخصي الذي كان يعمل على نظام MS-DOS للعمل على نظام Linux الذي يملك مزايا UNIX الأمنية نفسها.

3- Macintosh

مخدّمات Macintosh قليلة نوعاً ما ولكنها تتصرف تصرفاً مشابهاً لمخدّمات NT، وهي مخدّمات ذات واجهة تخاطبية بيانية، وتتطلب وجود سماحيات قراءة وكتابة للملفات والمجلدات، ويجري تحديد هذه السماحيات من خلال AppleTalk.

وبعض عمليات التحكم بالنفاذ من خلال مخدّم FTP متوفرة إذا كان Macintosh يشغّل AppleTalk.

4- Window NT

كما هي الحال في نظام UNIX فإن هذا النظام يملك مخدّم FTP كجزء منه، ويقدم أغلب الوظائف المتوفرة ضمن مخدّمات UNIX، وتهيئته تتم من خلال واجهة تخاطبية وليس من خلال لغة الأوامر. ولكن مخدّم Windows NT يختلف عن مخدّم UNIX في العديد من النواحي، مثلاً في نظام NT هناك مجلد وحيد مخصص ليكون مجلد العمل الافتراضي لأي مستخدم كان، بينما في نظام UNIX

يمكن أن يختلف مجلد العمل الافتراضي حسب المستخدم، وهذا المجلد هو المحدّد في ملف /etc/passwd.

يوضّح الشكل (5-4) نافذة التهيئة لخدّم FTP على نظام NT، حيث يمكن من خلال هذه النافذة التحكم بالعديد من الخواص مثل العدد الأقصى للمستخدمين المتصلين في آن واحد، وزمن بقاء الاتصال بدون عمل، ونرى من الشكل السابق أيضاً إمكانية تغيير الحساب العام إلى أي حساب آخر عادي، ولكن بما أن الحساب anonymous هو معيار متبع في الإنترنت (بصورة غير رسمية) فإن تغيير اسم الحساب العام قد لا يكون مستحسناً، إن المزايا المعروضة سابقاً غير موجودة في مخدّمات UNIX، وبالمقابل فإن الحماية في مخدّم NT تكون أقل قوة، فالتحكم بسماحيات القراءة والكتابة يحدث على مستوى تقسيمات القرص الصلب، ولا يمكن أن يتم على مستوى الملفات، كما أن NT لا تملك إمكانيات تمكنها من معرفة من يدخل إلى المخدّم، وبالنسبة لها كل المستخدمين هم إما مستخدمين anonymous وإمّا مستخدمين non-anonymous.

الشكل (5-4): تهيئة مخدّم FTP على نظام Windows NT

5-2-6 المعلومات التي يجب التشارك بها عبر خدمة نقل الملفات

بعد أن قمنا باستعراض أساسيات هذه الخدمة، سوف ننتقل الآن لعرض مبررات اختيار هذه الخدمة، وأسباب استخدامها، وما هي الاستراتيجيات التي يمكن اتباعها لتحديد ما الذي يجب أن نتشارك عليه وكيف. سنعرض هذه الأمور من وجهة نظر الإنترنت أولاً، ثم من وجهة نظر الإنترانت ثانياً.

1- التشارك عبر الإنترنت

عند الحديث عن المشاركة في الإنترنت فإن ذلك يعني أن الملفات ستصبح مشتركة على مستوى شبكة الإنترنت كلّها، وهناك العديد من النقاط التي يمكن مناقشتها في هذا الحالة.

الإعلام

يجب إعلام المستخدمين دوماً بوجود حساب عام مفتوح على الإنترنت من خلال إعلانات إلكترونية أو غير إلكترونية. إحدى الطرق السهلة نوعاً ما هي عرضُ إعلانٍ على صفحة الوب الخاصة بالمؤسسة، أو بإرفاق عنوان FTP بالمطبوعات التي تنشرها المؤسسة.

أنماط المعطيات

قبل اختيار المعطيات يجب الانتباه إلى أن أي شخص قد يتصل بهذا النظام، ولذلك يجب التأكد من أن المعطيات والملفات التنفيذية المشتركة جاهزة للاستخدام وخالية من الأخطاء. يمكن أن تكون هذه المعطيات المشتركة ملفات توثيق للمنتجات، أو ملفات المساعدة في حال حدوث الأعطال أو مشاكل سوء استخدام المنتجات. وإذا كانت الشركة تدير نوعاً من الأعمال التجارية فيمكن وضع قوائم بالأسعار ومعلومات عن المبيعات أو حتى السير الذاتية للعاملين في الشركة. نحصل بهذه الطريقة على نوع من الإعلام المجاني، ويجب عموماً أن يحتوي حساب FTP العام على كل ما تريد المؤسسة تعميمه.

أمور أساسية

أولاً: يجب وضع ملف فهرسة أو جدول بالمحتويات، وعادةً تكون أسماء هذه الملفات هي readme.txt أو TOC، كما يجب أن تضم هذه الملفات المعلومات الحديثة على الدوام عن محتويات الموقع حتى لا يفقد المستخدمون الاهتمام بالموقع.

ثانياً: يجب عدم إتاحة سماحيات الكتابة إذا لم يكن هناك سبب وجيه لذلك، إذ أن إتاحة الكتابة على النظام قد تجعل النظام عرضة للفيروسات أو للـ Internet worm.

ثالثاً: يمكن استخدام تقنيات الضغط لمجموعة معينة من الملفات التي تشترك بخصائص عامة، وذلك للتقليل من حجم القرص الصلب المستخدم لتخزين ملفات الحساب العام، وكذلك للتخفيف من عرض حزمة النقل عبر الشبكة وعلى المخدّم ، كما أن هذه العملية توفر على المستخدمين إجراء تعليمة "mget".

2- التشارك ضمن الإنترانت

المحاذير الأمنية التي تجب مراعاتها ضمن شبكة الإنترانت أقل من الحالة السابقة، ولكن من الضروري تحديد المعطيات الواجب التشارك بها عبر الحساب العام. إذ يمكن وضع أدوات برمجية عامة للاستخدام الداخلي، وهذه الطريقة فعّالة في وضع التطبيقات الضرورية في المؤسسة في موقع واحد يمكن للجميع النفاذ إليه ،كما يمكن أن نضع فيه الوثائق الداخلية مثل معايير العمل أو السياسات المتبعة في الشركة أو ذاتية العاملين أو ملاحظات عن المشاريع الحالية. ويجب الانتباه إلى نقطة مهمة وهي أن تكون الملفات الموضوعة في الحساب العام متوافقة مع مختلف أنظمة تشغيل المستخدمين.

5-2-7 أمن الشبكة وخدمة نقل الملفات

بنية نظام الملفات

يجب التأكد من أن الأجزاء الخاصة بالحساب العام معزولة تماماً ولا تحتوي على ملفاتٍ وبرامجَ تنفيذيةٍ غير ضروريةٍ. كما يجب التأكد أنه لا توجد أي اختصارات أو ارتباطات مع ملفات أخرى (لتجنب حدوث مشاكل في الحساب العام، لأن إجراء chroot مثلاً يضع الملفات المرتبطة في أماكن لا يستطيع المستخدم النفاذ إليها). كما يجب تجنب وضع أي ربط مع نظام ملفات الشبكة NFS ضمن مجلد الحساب العام.

عزل النظام

يجب عزل النظام جيداً إذا كان المخدّم موصولاً إلى الإنترنت، وذلك لتجنب الدخول إلى الإنترانت من خلاله، وعموماً يجب أن نسعى إلى التقليل من التقاطعات بين الإنترنت والإنترانت.

التحكم بالنفاذ إلى المخدّم

هناك نوعان من النفاذ إلى المخدّم ؛ النفاذ الفيزيائي والنفاذ البرمجي. فيزيائياً، أو من الناحية الجغرافية، يجب أن يكون نظام المخدّم موجوداً في مكان آمن، ويجب عدم السماح للأشخاص العاديين في الشركة بالوصول إلى هذا المكان، وذلك لتجنب أن يقوم أحدهم بتغيير بنية النظام أو إعطاء نفسه سماحيات أعلى. أمّا من الناحية البرمجية فلا داعي لإضافة الحسابات غير الضرورية، كما تجب مراقبة عملية الدخول إلى المخدّم وقراءة ملف تسجيل الدخول (Log File) جيداً.

قطع الاتصال بعد time-out

من المفضل تهيئة مخدّم FTP - إن أمكن ذلك - لقطع الاتصال بعد فترة معينة في حالة عدم القيام بأي عملية نقل، مما يقلل من مخاطر أن يترك المستخدم حاسوبه أثناء القيام بجلسة اتصال مع المخدّم ويترك النظام في حالة انتظار غير مجدية.

3-5 البريد الإلكتروني

إن أحد أهم أسباب الانتشار الواسع للبريد الإلكتروني وحصوله على شعبية كبيرة مع محافظته على آلية عمله هو بساطته. وعلى العكس من الأدوات والبرمجيات التي ما أن وجدت طريقها إلى بيئة التطبيقات المكتبية حتى قلّ استعمالها أو أهملت كلياً بسبب صعوبتها وصعوبة فهم التوثيق الفني المرفق بها، فإن الاعتماد على البريد الإلكتروني كخدمة أساسية في شبكات الإنترانت يأتي بفضل المزايا الثلاث التالية:

- توفير الوقت (توزيع آني للأخبار).
- توفير التكلفة (تكلفة نسخ مختلف أنواع المستندات الورقية المتداولة).
- سهولة إتقان التعامل معه حتى من قبل الأشخاص العاديين.

إن تطبيق البريد الإلكتروني هو وسيلة اتصال سريعة فعّالة من الممكن اقتناؤها بتكلفة معقولة، وهو من التطبيقات التي تجب إضافتها إلى قلب الخدمات في شبكة الإنترانت لأي مؤسسة تعاونية.

لقد كانت خدمة البريد الإلكتروني مهملة (كما كانت حال نظام UNIX بسبب افتقاره للواجهة التخاطبية الجيدة)، بسبب أن أغلب تطبيقات البريد الإلكتروني كانت مبنية على نظام UNIX وتعمل من خلال العديد من الأوامر النصية. وإذا نظرنا إلى ما كانت عليه تقنيات الحواسيب وكيفية تعامل المستخدمين معها في السبعينيات والثمانينيات فيمكننا أن نستنتج أن البريد الإلكتروني قد نشأ في البداية بهدف تسهيل الاتصالات عبر مناطق واسعة جغرافياً ضمن شروط التكلفة المنخفضة والسرعة

المقبولة وليس كأداة للترفيه أو التسلية. وقد تطورت مخدّمات البريد الإلكتروني وبرامج الزبون الخاصة بها في السنوات الماضية ليصبح التعامل معها أكثر سهولة، ومن ثم لتصبح هذه الخدمة أكثر انتشاراً.

5-3-1 طريقة العمل

تعتمد البنية التحتية للبريد الإلكتروني على بروتوكول SMTP (Simple Mail Transfer Protocol). ينتمي هذا البروتوكول إلى الطبقة السابعة في معيار ISO/OSI، حيث أن خدمة البريد الإلكتروني تقع في طبقة التطبيقات من وجهة نظر بنية الشبكة.

يعمل مخدّم البريد الإلكتروني عند استقبال رسالة ما على تحويل أحرف نص الرسالة إلى سلسلة أحرف نظامية ويرسلها إلى الوجهة المطلوبة وفق العنوان المحدد في الرسالة. بعد ذلك تصل الرسالة إلى مخدّم بريد إلكتروني آخر على العنوان المستقبل، ليقوم هذا المخدّم بالتحويل العكسي لأحرف الرسالة وتسليمها للمستقبل.

عنونة البريد الإلكتروني

يتألف عنوان البريد الإلكتروني من جزأين أساسيين يفصلهما المحرف '@' مثلاً:

user-name@Computer-Name.Domain-Name

على يسار المحرف '@' نجد اسم الحساب الذي يستخدمه المستقبل لاستقبال رسائله الإلكترونية عليه، وعلى اليمين نجد اسم الحاسوب المضيف (أي مخدّم البريد الإلكتروني عند المستقبل)، ومن ثم اسم المجال الذي ينتمي إليه هذا الحاسوب.

ملاحظة 1

لتحصل أي شركة أو مؤسسة على اسم مجال واحد مثل fruitbat.com أو flyingmonkey.com بدلاً من عنوان الإنترنت المشابه لـ 172.25.1.6 وذلك لتعلن عن وجودها على الإنترنت، يجب طلب هذا العنوان من شركة interNIC (www.internic.net)، وهي شركة مرخصة من الحكومة الأمريكية لإدارة وتنظيم أمور العنونة على الإنترنت. يمكن أن تجري هذه العملية إلكترونياً عبر الإنترنت بزمن صغير، حيث يملأ طلب التسجيل في نموذج إلكتروني مقابل دفع مبلغ معين، ولكن لسوء الحظ أدّى هوس الحصول على العناوين على الإنترنت، إلى حجز كل ما قد نتخيله من أسماء (من dink.com إلى sausge.com وكل ما بينهما من أسماء). وإذا أردنا الحصول على عنوان يبدأ بـ cyber أو inter يلزمنا الكثير من الإبداع لاختراع عنوان لم يسبقنا إليه أحد، ومن المفضل القيام ببعض إجراءات البحث عن الأسماء التي أخذت والتي لم تحجز بعد، وذلك لتوفير الوقت وتجنب العديد من المتاعب.

ملاحظة 2

أحد الطرق المستخدمة لتحديد فيما إذا كان اسمٌ ما محجوزاً أم لا هي في استخدام تعليمة UNIX: whois، وذلك عن طريق الدخول إلى حساب على نظام UNIX موصول إلى الإنترنت ومن ثم كتابة التعليمة whois متبوعة باسم المجال المطلوب التحقق منه. عندها يصل الطلب إلى قواعد المعطيات في InterNIC ويجري البحث عن اسم المجال المطلوب. على سبيل المثال إذا كنا نبحث عن وجود الاسم interactive.com فسيكون الرد:

```
bash$whois intraactive.com
IntraActive, Inc. (INTRAACTIVE-DOM)
888 17th Street, NW Suite 1200
Washington, DC 20006

Domain Name: INTRAACTIVE.COM

Administrative Contact:
Garrett, David (DG215) dave@ID1.COM
```

```
202-667-7048
Technical Contact, Zone Contact:
Simon, Richard (RS2599) simon@INTRAACTIVE.COM
202-667-7048 (FAX) 202-667-7055
Billing Contact:
Majersik, Cliff (CM235) cliff@ID1.COM
202-331-8495

Record last updated on 09-Jul-96.
Record created on 21-Apr-96.

Domain servers in listed order:

NS.INTRAACTIVE.COM 206.55.46.10
NS2.INTRAACTIVE.COM 206.55.46.103


The InterNIC Registration Services Host contains ONLY Internet Information
(Networks, ASN's, Domains, and POC's).

Please use the whois server at nic.ddn.mil for MILNET Information.
bash$
```

وإذا أردنا البحث عن matzohballs.com فسيكون الرد مشابهاً لما يلي:

```
bash$ whois matzohballs.com

No match for "MATZOHBALLS.COM".

The InterNIC Registration Services Host contains ONLY Internet Information
(Networks, ASN's, Domains, and POC's).

Please use the whois server at nic.ddn.mil for MILNET Information.
```

ملاحظة 3

سنوضح فيما يلي معنى اللاحقة الموجودة في أغلب عناوين البريد الإلكتروني مثل: com. أو org. وغيرها من اللواحق. فلتتبع أثر أي شيء وتوفير إمكانيات عنونة وحيدة صُنفت العناوين حسب نوع النشاط الذي تقوم به الشركة صاحبة العنوان. فتأخذ اللواحق التالية (في الولايات المتحدة الأمريكية) والتي تسمى المجال ذا المستوى الأعلى الدلالات المبينة في الجدول (5-2).

وكما ذكرنا سابقاً، تُستخدم أسماء المجالات بدلاً من عناوين الإنترنت (عناوين IP) الصعبة الاستخدام والتذكر. تأخذ هذه العناوين شكل أربع مجموعات تتألف كل منها من ثلاث خانات عشرية كحد أقصى مثل العنوان: 172.25.1.8.

من الممكن طبعاً إرسال البريد الإلكتروني باستخدام عناوين IP، ولكن هذه الطريقة ستكون مزعجة حتماً، والطريقة المتبعة حالياً هي إسناد العنوان المؤلف من تتالي عدة مجالات تفصلها النقطة '.' لكل عنوان IP، مما يسهّل في حفظ العناوين واستخدامها ببساطة وسرعة.

.com	المؤسسات ذات الأغراض الربحية.
.org	المؤسسات ذات الإراض غير الربحية.
.gov	المؤسسات الحكومية.
.net	موقع مزود بحواسب تستخدم للحفاظ على الإنترنت.
.edu	معهد تعليمي.
.mil	المواقع العسكرية في الولايات المتحدة الأمريكية.

الجدول (5-2): معنى اللواحق المستخدمة في عناوين البريد الإلكتروني

ترويسة رسالة البريد الإلكتروني

هناك العديد من الحقول التي يمكن أن تُلحق برسالة البريد الإلكتروني وهي أعقد من عنوان المرسل وعنوان المستقبل المستخدمان في الرسائل البريدية العادية، ولكن ليس من الضروري كتابة كل هذه الحقول، فالحقل الضروري الوحيد لوصول الرسالة هو عنوان المستقبل. يبين الشكل (5-5) رسالة بريد إلكتروني نموذجية. وفيما يلي الحقول التي يجب الاهتمام بها عند إرسال رسالة بريد إلكتروني.

الحقل To

يحتوي هذا الحقل عنوان البريد الإلكتروني للشخص المستقبل، وفي أغلب الحالات التي يقع العنـوان فيها ضمن نفس مجال الذي ينتمي إليه المرسل فلا داعـي لتحديـد اسـم المجـال، أي لكتابـة الجـزء الذي يلي المحرف '@'، وذلك بحسب برنامج البريد الإلكـتروني الزبـون المستخدم، ويسـمى هـذا الحقل أحياناً بحقل "Message To" أو "Mail To".

الحقل From

يضم هذا الحقل عنوان البريد الإلكتروني للمرسل، وهو غير ضـروري لأن برنـامج الزبـون يقـوم بملئـه تلقائياً.

الحقل Subject

يجب أن يحوي هذا الحقل وصفاً مقتضباً (20–30 حرف) للرسـالة، ويمكـن أن يُسـمى هـذا الحقـل باسم: عنوان الرسالة أو ببساطة: الرسالة. ويجب اختيار محتوى هذا الحقل بعناية لأن معظم الناس يقررون قراءة الرسالة أو عدم قراءتها اعتماداً على الموضوع.

الحقل CC

حروف اسم هـذا الحقـل هـي اختصـار لـ (Carbon Copy)، ويحتـوي عنـاوين البـريد الإلكـتروني لمستقبلين إضافيين ؛ حيث تصل نسخة من الرسالة إلى جميع هذه العناوين.

الحقل BCC

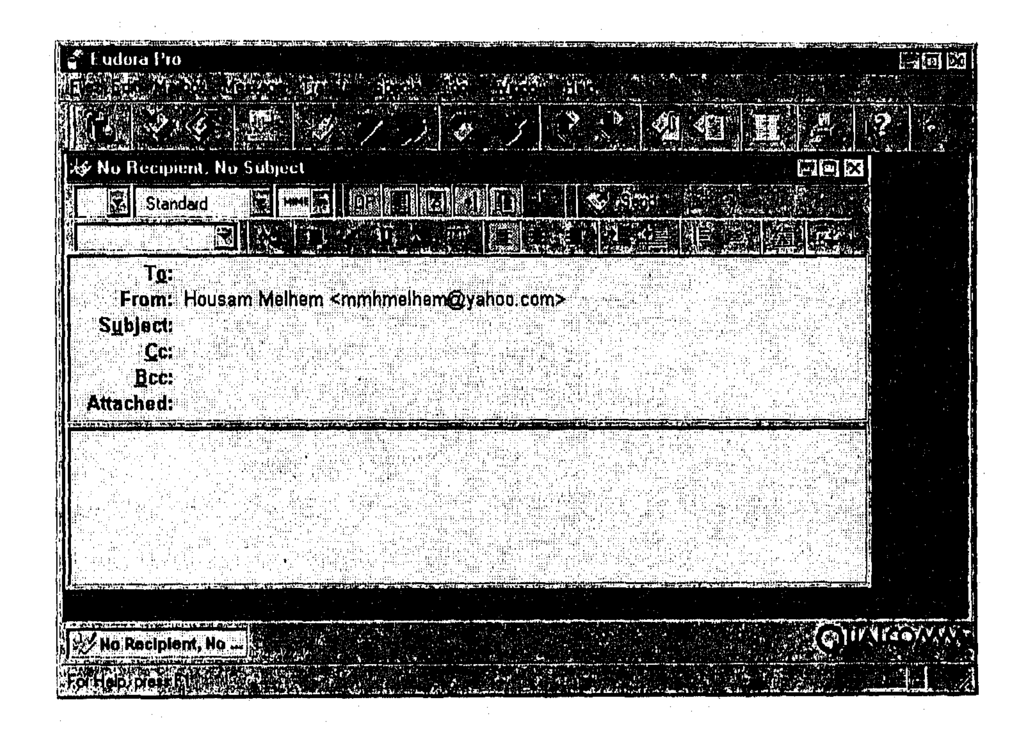
في العديد من برامج الزبون يكون هذا الحقل مخفيـاً ويجـب القيـام ببعـض العمليـات للوصـول إليـه، واسمه يأتي من اختصار (Blind Carbon Copy)، ويضم عناوين إضافية لإرسال الرسالة ولكـن بـدون أن يعلم بذلك الشخص الأول الذي سترسل إليه الرسالة، وعلى الرغم من أن استعمالات هـذا الحقـل قد تكون شرعية إلا أن العديد من المستخدمين قد يستخدمونه لأغراض غير شرعية.

الحقل Attachment

بعض التطبيقات لا تقدم هذا الحقل الذي يسمح بإرفاق مستند كامل مع الرسالة.

حقل التاريخ

لا يظهر هذا الحقل في أغلب تطبيقات البريد الإلكتروني، وهو مطلوب من قبل المخدّم لمعالجة البريد الإلكتروني، ويجب التحقق من أن ساعة الحاسوب الذي نعمل عليه صحيحة لنضمن صحة وقت وتاريخ الرسالة.



الشكل (5-5): رسالة إلكترونية

5-3-2 فوائد ومزايا البريد الإلكتروني

من فوائد البريد الإلكتروني في المحيط التعاوني إمكانية إرسال الرسائل بسرعة وسهولة إلى أي عدد من المستخدمين أو الزبائن، وقد يؤدي دمج مختلف وظائف البريد الإلكتروني المتطورة في محيط العمل التعاوني إلى إغناء إنتاجية نظام المؤسسة، وفيما يلي بعض مزايا خدمة البريد الإلكتروني:

آ- العنوان البديل

لنفترض أن الشركة تملك مكتباً للدعم الفني يعمل فيه العديد من العاملين ذوي الكفاءة العالية، وعادةً ما يحصل العاملون على الدعم الفني المطلوب إما عن طريق معرفتهم بشخص ما في مكتب الدعم الفني فيعتمدون حصراً على هذا الشخص، أو عن طريق التراسل من خلال البريد الإلكتروني مع أشخاص يمكن تصنيفهم كمساعدين فنيين في مختلف فروع الشركة. هذه الطريقة في الحصول على الدعم غير مجدية من وجهة نظرٍ تعاونيةٍ، كما أنها محبطة لكل من المستخدم ومجموعة الدعم الفني، وباستعمال تقنية العنوان البديل (Aliasing) يمكن تخصيص حساب بريد إلكتروني وهمي، أي أنه لا يخص شخصاً محدداً، مثلاً support@company.com وذلك لاستخدامه كعنوان معياري للدعم الفني، حيث يجمع هذا العنوان كل الرسائل ويوجهها إلى مستخدم معين، وليكن مثلاً david@company.com. توفّر هذه الطريقة الكثير من النقاش حول ضرورة تعميم عنوان جديد للحصول على الدعم الفني، كما أنها تحافظ على تدفق طلبات العمل والأسئلة وما شابه ذلك مما يعزز من الإنتاجية التعاونية.

ب- تبادل الرسائل عن بعد

بالنسبة للشركات والعاملين فيها المستغرقين في حركة التعامل مع الزبائن وعقد الصفقات ومعالجة المستندات، فإن التأكد من أن العاملين في الشركة على صلة دائمة بالمدراء وبمجموعات الدعم الفني والزبائن أصبح من الضرورات القصوى. فالبريد الإلكتروني يسهل الاتصالات وخاصةً عندما يترافق مع

استخدام التقنيات الحديثة الجديدة مثل الهواتف الخليوية والـ Pagers. فعندما يُرفق البريد الإلكتروني ببرمجيات مناسبة يمكن من خلالها تمرير البريد القادم إلى الخدمة المناسبة، يصبح بالإمكان إرسال البريد إلى عنوان معين تمكن من خلاله قراءة الرسائل على شاشة الحاسوب أو من خلال الهاتف الخليوي أو الـ Pager.

ج- عرض حزمة النقل المنخفض

على النقيض من خدمات الإنترنت الأخرى، مثل خدمة الوب التي تمكّن من نقل ملفات HTML والتي أصبحت مزودة بالصور والصوت وغير ذلك من الملفات ذات الحجوم الكبيرة، فإن خدمة البريد الإلكتروني تتطلب حجماً صغيراً من عرض حزمة النقل. إذ يكفي بالنسبة لمكتبٍ صغيرٍ أن يستخدم موديماً بسرعة نقل 28.8KBps أو شبكة ISDN، ويمكن لشركة كبيرة أيضاً استخدام شبكة ISDN أو خط نقل T-1 إذا كانت خدمة البريد الإلكتروني هي الخدمة الوحيدة المعتمدة.

د- الاستخدامات المكتبية للبريد الإلكتروني

كان لظهور خدمة البريد الإلكتروني الأثرُ الأكبرُ على البيئة المكتبية من خلال التغيير الجذري للعديد من المهمات التقليدية الأساسية في المحيط التعاوني. وقد يكون أكبر تغيير هو في حقل المذكرات المكتبية، فلنشر إعلان أو تغيير في سياسة الشركة أو ما شابه ذلك، كان على المدير اتباع عدد معين من الخطوات ليضمن أن جميع العاملين المعنيين بالأمر أصبحوا على علم. أمّا باستخدام البريد الإلكتروني فإنه يمكن القيام بجميع هذه الخطوات بسهولة وسرعة. لكن إرسال المذكرات ليس المجال الوحيد المستفيد من البريد الإلكتروني، حيث تستخدم الشركات اليوم هذه الخدمة على شبكات الإنترانت للقيام بالعديد من النقاشات وللتنظيم الزمني للاجتماعات، ولطلب التجهيزات المكتبية وغيرها، ولتقديم تقارير المبيعات واللوائح الزمنية، حيث يسمح البريد الإلكتروني بتخليص مكاتب الشركة من التعامل الورقي إلى حد ما، كما أنه طريقة مثالية للتنسيق بين جميع العاملين في الشركة.

هـ- التشارك على الملفات

إضافةً إلى إمكانية إرسال الرسائل النصية يمكن استخدام البريد الإلكتروني كوسيلة للتشارك على المستندات أو البرامج أو أي نوع من أنواع الملفات، حيث يمكن إرفاق أي ملف مع رسالة البريد الإلكتروني. وعلى الرغم من أن الملف يخضع لعلمية ترميز من قبل برنامج الزبون قبل الإرسال إلا أن العديد من هذه البرامج يقوم بالترميز وفك الترميز، ولذلك فإن مسألة التوافق لا تسبب أية مشكلة.

و- mailbots

mailbot هو عبارة عن موقع للرد التلقائي على رسائل البريد الإلكتروني، حيث يقدم إمكانية إعطاء أجوبة بسيطة لأسئلة بسيطة (كالسؤال عن كيفية تثبيت Netscape على حاسوب معين، أو طلب إجازة). يجري هذا الأمر عن طريق إعداد قائمة أسئلة تسمى FAQ (Frequently Asked Questions) توضع في mailbot.

فإذا أراد شخص معين في البيت الأبيض على سبيل المثال معرفةَ كيفية تثبيت برنامج Netscape فيمكنه الإرسال إلى عنوان netscape-setup@whitehouse.gov، ليقوم المخدّم عندئذٍ بإرسال رسالة تتضمن الـ FAQ تلقائياً. ومن الممكن بناء mailbot للإجابة على العديد من الأسئلة وليس على سؤال واحد، كما يمكن ربطه مع قواعد المعطيات بحيث يقوم mailbot بالبحث فيها تلقائياً وإعادة المعلومات المطلوبة بدون أي تدخل بشري.

ز- قوائم البريد

هي برامج (تسمى أحياناً بـ listservs) تعمل على المخدّم، وتستخدم عادة لإجراء مناقشة بين عدد كبير من المستخدمين، وتفيد أيضاً في نشر المعلومات في المحيط التعاوني.

تتألف القائمة من عنوانين، العنوان الفعلي للقائمة وعنوان الإشراف، ويمكن لأي شخص أن يرسل رسالة لطلب التسجيل في القائمة وذلك باستخدام عنوان الإشراف، أما الرسائل المرسلة إلى العنوان الفعلي فإنها تُرسل تلقائياً إلى كل المسجلين.

إضافةً إلى التسجيل في القائمة يمكن أيضاً إلغاء التسجيل أو القيام بوظائف أخرى كطلب آخر تسع رسائل مثلاً، أو أي رسالة خاصة تحقق شرط ورود كلمة معينة فيها. وإذا كانت القائمة كبيرة يمكن تلخيصها وإرسالها تلقائياً (يومياً أو أسبوعياً) بدلاً من إرسال الرسائل عند وصولها.

هناك نوعان من قوائم البريد: مرؤوسة وغير مرؤوسة، في القوائم المرؤوسة يمكن لشخص واحد فقط وهو الرئيس إرسال الرسائل إلى قائمة البريد، أما في حالة القوائم غير المرؤوسة فجميع المسجلين في القائمة بإمكانهم إرسال الرسائل إلى القائمة.

تستخدم الشركات قوائم البريد لإبقاء العاملين على اطّلاع دائمٍ على المعلومات المتغيرة (تغير الأسعار على سبيل المثال)، ويمكن حفظ هذه المعلومات في قاعدة معطيات معينة، ولكن سيضطر العاملون عندئذٍ إلى التحقق الدوري من تغير المعلومات، في حين تقوم قائمة البريد بإعلامهم تلقائياً عند حدوث أي تغير، كما يكن التسجيل في قوائم أخرى للحصول على معلومات من مؤسسات خارجية عبر الإنترنت. وليس من الضروري أن تكون القائمة كبيرة لتصبح مفيدة، إنما يمكن إعداد قائمة بريد لتخديم قسم واحد في الشركة.

ح- الاتصالات عبر الشبكات واسعة النطاق

بالنسبة للشركات التي تملك مكاتبَ في مواقع متباعدة، أصبح البريد الإلكتروني حاجة ضرورية، فبدلاً من استخدام البريد العادي الذي قد يستغرق أياماً أو أسابيع للوصول إلى العنوان المحدد، فإن البريد الإلكتروني يقدّم خدمة أسرع بتكلفة منخفضة وذلك عبر الشبكات واسعة النطاق.

5-3-3 مخدّم البريد الإلكتروني

إن تشغيل مخدّم للبريد الإلكتروني ليس مهمة صعبة عند تصميم وبناء شبكة الإنترانت، وللتعامل مع مخدّمات البريد الإلكتروني يجب فهم بعض المبادئ الأساسية والمصطلحات والمزايا خلال مرحلة تصميم الإنترانت، مما يمكننا من تقييم احتياجات الشركة مقارنة مع المصادر المالية المتوفرة.

هناك العديد من أنواع مخدّمات البريد الإلكتروني المتوفرة، وبالنسبة لبيئة شبكة محلية أو شبكة واسعة النطاق يمكن استخدام المخدّمات المتوفرة تجارياً مثل GroupWise أو Microsoft Mail أو AppleTalk.

إن مخدّم GroupWise متوفر للعديد من الحواسيب الشخصية أو الماكينتوش، ولكن بما أن هذه المخدّمات لا تستخدم المعايير المعروفة فإنها لا تستطيع التواصل مع مخدّمات البريد الإلكتروني في الإنترنت، حيث تستخدم مخدّمات الشبكات المحلية والشبكات واسعة النطاق بروتوكولاً خاصاً بها بدلاً من استخدام بروتوكول SMTP أو POP3. ويمكن مكاملة مخدّمات GroupWise و Microsoft Mail في البريد الإلكتروني على الإنترنت وذلك عن طريق تطوير البرمجيات المناسبة لذلك.

بروتوكولات الإرسال والاستقبال

يعتبر بروتوكول POP3 معيارياً في استقبال البريد الإلكتروني، فباستخدام هذا البروتوكول يستطيع المخدّم التعامل مع برنامج الزبون على حساب المستخدم، حيث يبقى البريد الإلكتروني الخاص بمستخدم معين على المخدّم في حساب هذا المستخدم إلى أن يدخل المستخدم إلى حسابه ويستخلص بريده. وعلى الرغم من أن بروتوكول POP3 من أكثر البروتوكولات استخداماً إلا أن له سيئة لا يستهان بها، فهو يعمل من جهة المستخدم فقط، إذ يرسل البريد إلى حاسوب المستخدم وهناك تمكن معالجته وحفظه على هذا الحاسوب فقط، ومن ثم يستحيل الوصول إليه من حاسوب آخر لمعالجته أو قراءته مرة أخرى.

بروتوكول IMAP هو بروتوكول حديث لاستقبال الرسائل مقارنةً مع POP3، حيث يعمل هذا البروتوكول من جهة المخدّم، ويسمح بمعالجة البريد الإلكتروني على المخدّم، ومن ثم يمكن الحصول عليه من أي حاسوب كان.

بروتوكول SMTP هو البروتوكول المعياري لإرسال البريد الإلكتروني، وكل حاسوب مضيف للبريد الإلكتروني يملك مخدّم SMTP سواء أكان بروتوكول الاستقبال هو POP3 أو IMAP. يقوم هذا البروتوكول بفرز وتوجيه الرسائل إلى العنوان المناسب، وفي حال كون الحاسوب المضيف لمخدّم SMTP يحمل برمجيات مثل Pine أو ELM، فيمكن الحصول على الرسائل عن طريق النفاذ إلى حساب ما على الحاسوب المضيف بدلاً من استخدام مخدّمات POP3 أو IMAP. وبما أن البروتوكولات الثلاثة IMAP وPOP3 و SMTP هي بروتوكولات معيارية عامة فهي متوفرة في جميع البنى المادية والبرمجية.

خيارات المخدّم

على الرغم من وجود المئات من الخيارات المتوفرة عند البحث عن برامج الزبون، فإن مجال مخدّمات الـ SMTP ليس بهذا الاتساع. لكنّ هناك عدداً من الخيارات الجيدة المتوفرة على مختلف البنى المادية والبرمجية.

Post.Office .1

يعمل هذا المخدّم ذو المزايا القوية ضمن بيئة نظامي Window NT و UNIX، وقد تم تطويره بناءً على المعايير العالمية لبروتوكولات الإنترنت. وفي تصميم الإنترانت هناك هدفان تجب مراعاتهما عند بناء النظام، وهما الفعالية والوثوقية. وبالطبع فإن Post.Office صُمم ليلائم المتطلبات المتزايدة للتراسل الإلكتروني ضمن المحيط التعاوني، وهذا المخدّم يحتوي على مزايا عالية فيما يخص الإشراف والأمن للتخفيف من حدة المشاكل في هذا المجال.

يقوم مخدّم Post.Office بالعديد من الأمور بجودةٍ مرضية مع القليل من الأخطاء، ويحتوي على العديد من الأدوات التي تجعله الخيار الأمثل كأداة مساعدة للاتصالات المكتبية. ويملك هذا المخدّم خصوصاً أدوات للتهيئة عن بعد والإجابة التلقائية، ومخدّمات POP3 و SMTP و Finger متكاملة مع نظامه، مما يسمح بحرية الاختيار عند تهيئة وتعزيز قدرات الاتصالات في الإنترانت. ومن أهم مزايا Post.Office ميزة الإدارة عن بعد على أساس الوب، وهي تسمح بتغيير أي ميزة من وظائف المخدّم وذلك من أي موقع يمكن النفاذ منه عبر الوب.

يمكن الحصول على المزيد من المعلومات أو الحصول على المخدّم نفسه بنسخة كاملة تعمل لمدة 45 يوماً من الموقع www.software.com.

2- مخدّم Netscape للبريد الإلكتروني

وفقاً لشركة Netscape فإن هذا المخدم هو حل SMTP/IMAP/MIME طبيعي للتراسل يعمل مع أنظمة SMTP الأخرى المتوافقة، وهو يقدّم خدمة توصيل الرسائل على نحو أسرع وأعلى جودةً. ويقدّم أساساً العمود الفقري للتراسل التعاوني عالي الأداء، كما أنه متماسك ويمكن الاعتماد عليه في المؤسسات التجارية.

يعمل هذا المخدّم على بيئة Windows NT/Alpha و UNIX، ويدعم بروتوكول IMAP4 (Internet Mail Access Protocol 4)، ويقدم مزايا للإدارة المركزية العليا. وتتكامل هذه المجموعة البرمجية مع مجموعة SuitSpot Netscape، مما يعني أنه يدعم لغة Java و JavaScript الأمر الذي يضيف مستوىً وظيفياً جديداً لخدمات الإنترانيت.

ولمزيد من المعلومات حول هذه المجموعة البرمجية تمكن زيارة المواقع:

http://www.collabra.com/products/index.htm

http//www.home.netscape.com/newsref/pr/newsrelease124.html

3- مخدّم *Microsoft Exchange Server*

إن الإمكانيات والمرونة التي يقدّمها هذا المخدّم متنوعة جـداً، وبما أن Exchange يدعـم الكثـير مـن المعايير القياسية مثل X.400، SMTP، MIME، MAPI، TCP/IP، PPP، SLIP، X.509، فمن المفيد دمج Exchange في أي نظام مثبت حالياً على شبكة الإنترانت التعاونية، أو حتى إحلاله محل أي نظام على نحوٍ كامل بهدف بناء نظام Exchange قائم بحد ذاته إذا رغبنا بذلك.

ويمكن ملاحظة النقص في الملفات المساعدة بالنسبة لبعض المزايا الشائعة مثل POP3، HTTP، NNTP، LDAP. ووفقاً لممثلي شركة Microsoft، فإن دعم هذه الخدمات هو قيد التنفيذ حالياً (؟) ومن المفروض أن تحتويه النسخ القادمة. وعلى الرغم من أن هذا النقص يمثل، على نحوٍ ما، عقبة إذا أردنا تأهيل خدمة مثل POP3 مع انتظار الإصدار المتأخر للملفات الدعم، فإنه يمكن الحصول على المزيد من المعلومات حول Exchange من الموقع:

http://www.microsoft.com/exchange/interexch.htm

في حال كون الشركة صغيرةً أو عند عدم الرغبة في إنفاق الأموال الكثيرة في البداية فإن الخيار المثالي في هذه الحالة قد يكون مخدّم Seattle Lab الذي يعمل ضمن بيئة Windows 95 ويدعم البروتوكولات SMTP/POP3، وهو متوفر بكلفة معقولة كما أنه شائع الاستخدام، وهذا المنتج المسمى Slmail95 الذي على الرغم من واجهته التخاطبية الضعيفة نوعاً ما، فأنه يسمح ببناء قوائم للبريد، ويدعم الأسماء البديلة، وخدمة mailbots، كما يمكن أن يعمل من خلف الجدار الناري بمعنى أنه يراعي الناحية الأمنية .

وللحصول على معلومات أكثر عن هذا المنتج يمكن زيارة الموقع:

http//:www.cloud-nine.co.uk/slmail95.htm

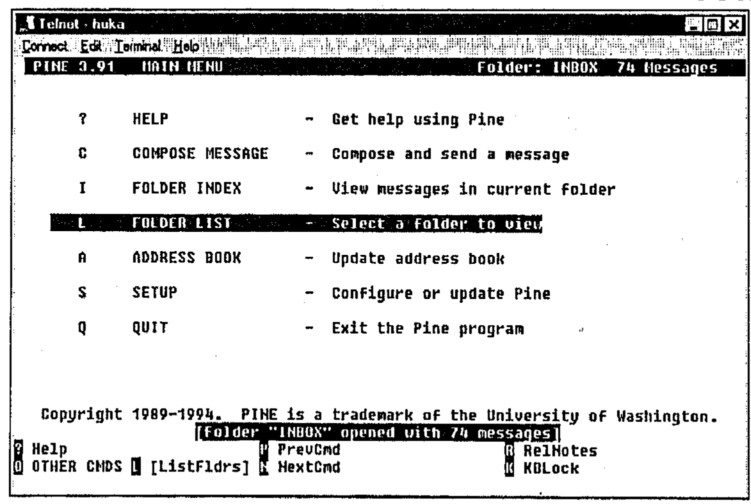
5-3-4 برامج الزبون

هناك المئات من تطبيقات برامج الزبون والعديد منها مجاني، وتقوم معظم هذه التطبيقات بالعمل الأساسي نفسه تقريباً، وسوف نقوم فيما يلي بجولة سريعة على الأدوات الشهيرة والمتميزة بعضها عن بعض.

Pine -1

برنامج زبون للبريد الإلكتروني، طوِّر في جامعة Washington في Seattle عام 1989، ويستخدم من قبل المستخدمين الذين يملكون حسابات على مخدّم البريد الإلكتروني (هذا التطبيق شائع الاستخدام بين المبرمجين)، ولا يقدم هذا التطبيق واجهة تخاطب بيانية إلا أنه يتمتع بالعديد من المزايا، كما أنه سهل الاستعمال نسبياً.

باستخدام هذا التطبيق يمكن الرد على الرسائل، وتوجيه البريد، وإرسال نسخ أو "CC" إلى عناوين أخرى، وبناء قوائم للبريد، وتنظيم الرسائل في أي عدد من المجلدات. ويمكن أيضاً باستخدام هذا التطبيق الحصول على البريد من أي موقع كان، حيث أن هذا التطبيق يعمل على المخدّم، ولا يستخدم بروتوكول POP3.



الشكل (5-6): تطبيق Pine

Eudora -2

هذا التطبيق مزود بالعديد من المزايا أيضاً ويخرج بإصدارات تعمل على الحواسيب الشخصية والماكينتوش، وهو متوفر تجارياً ومجانياً. لكن النسخة التجارية تحتوي على العديد من المزايا الإضافية مثل التدقيق الإملائي، أمّا الجانب السيئ لهذا التطبيق فيكمن في كونه يعمل على حاسوب المستخدم، بمعنى أنه لا يسمح بمعالجة البريد إلا بعد نقله من المخدّم، ومن ثم لا يمكن الوصول إلى البريد من أي حاسوب آخر بعد استقدامه من المخدّم.

SPRYMail -3

يملك هذا التطبيق ميزة رائعة تستحق الذكر، وهي أنه يسمح بقراءة البريد قبل استقدامه من المخدّم، وهذه الميزة تسمح بحذف الرسائل غير المرغوبة، أو الرد فوراً على الرسائل. وإذا تركنا الرسائل على المخدّم يصبح بالإمكان الحصول عليها من أي مكان يمكن النفاذ منه إلى المخدّم. تقوم برامج الزبون الأخرى بهذه الوظيفة ولكن ليس بالوضوح ذاته الذي يقوم به هذا البرنامج، ولكن SPRYMail لا يملك مرونة تطبيق Pine كما أنه لا يجاري التصميم البديهي لتطبيق Eudora.

4- تطبيق GroupWise

هو تطبيق شائع الاستخدام في بيئة الشبكات المحلية، ويمكن تطويره ليتوافق مع البريد الإلكتروني عبر الإنترنت، وهو ليس بغنى تطبيق Eudora كما أنه يفتقد إلى المزايا التي يفضلها المستخدمون عبر الإنترنت. على سبيل المثال يسمح تطبيق Eudora بتغيير كلمة مرور البريد الإلكتروني، وهو من الأمور التي يُشجّع المستخدمون عبر الإنترنت على إجرائها دورياً، ولكن باستعمال GroupWise فإن كلمة المرور للبريد الإلكتروني هي كلمة المرور لحاسوب المستخدم.

5- تطبيق *Netscape Mail*

تطبيق متعدد المزايا وإن لم يكن مثالياً، ولكن بالنسبة للتطبيقات التي جرى إصدارها حتى الآن فهذا التطبيق يقارب المثالية، إضافةً إلى أن هذا التطبيق مدمج مع مجموعة مستعرض Netscape البرمجية. الميزة الأساسية التي تميز هذا التطبيق هي أنه يمكن من خلاله تضمين الملفات المتعددة الوسائط مثل الفيديو أو النصوص أو أي شيء يمكن إدخاله إلى ملفات HTML ضمن رسائل البريد الإلكتروني. ولكن هذه التقنية الجديدة ليست بالأمر الكبير بالرغم من أن الفكرة كانت رائعة من قبل شركة Netscape، حيث قامت هذه الشركة بأخذ التقنيات التي جعلت من مستعرض Netscape يحتل مكانته البارزة تجارياً، وقامت بتطبيقها على نظام البريد الإلكتروني.

إن اختيار برنامج الزبون الأمثل لشبكة الإنترانت يتعلق بما نرغب في تحقيقه من خلال توفير خدمة البريد الإلكتروني، ويمكن تجريب التطبيقات الخمسة سابقة الذكر. فإذا كنا نرغب بإضافة الصوت أو الصور إلى رسائل البريد الإلكتروني فإن Netscape Mail هو الخيار المناسب في هذه الحالة، أما إذا أردنا تطبيقاً متعدد المزايا وسهل الاستخدام فإن تطبيق Eudora قد يكون الخيار الأفضل. نعرض في الجدول (5-3) مقارنةً بسيطة لمزايا التطبيقات الخمسة السابقة.

Netscape	GroupWise	SPRYMail	Eudora	Pine	الميزة
*	محدودة	*	*		POP3
محدودة					IMAP
*	*	*	*	*	الأسماء المستعارة
				*	المجلدات
	*		*	محدودة	الفلترة
		*		*	النفاذ عن بعد
	*		*	*	التدقيق الإملائي
*	*	*	*		الاستخدام المكتبي
*		*	*	*	البحث

الفرز	o	*			*
إلحاق المستندات	محدودة	*	*	*	*

الجدول (5-3): مقارنة بين برامج الزبون لخدمة البريد الإلكتروني

5-4 المؤتمر الفيديوي

في الفقرات السابقة رأينا الخدمات الأساسية الواجب على أي شبكة إنترانت أن تقدمها، وسنتناول في هذه الفقرة تطبيقاً خاصاً هو المؤتمر الفيديوي (Video Conferencing). فعلى الرغم من أن هذا التطبيق ليس من الخدمات الجوهرية التي يجب أن تقدمها الإنترانت إلا أنه يقدم وسائل عملية للاتصال بين العاملين في الشركة والزبائن. ولتقييم إيجابيات وسلبيات المؤتمر الفيديوي في الإنترانت والإنترنت يجب أن نأخذ بعين الاعتبار قيود عرض حزمة النقل (Band Width)، وكذلك المتطلبات الفيزيائية والبرمجية على كلٍّ من المخدِّم والزبون، إضافةً إلى تكلفة كل حاسوب نريد تزويده بهذه الخدمة. وفيما يلي سنقوم بمناقشة تحقيق هذا التطبيق على أرض الواقع ومدى جدواه في أن يكون أداة اتصال عملية على شبكة الإنترانت.

5-4-1 التعريف بالمؤتمر الفيديوي في الزمن الحقيقي

ظهر المؤتمر الفيديوي كفكرة قابلة للتطبيق من خلال النموذج المسمى بنموذج "الغرف" الذي يتطلب أن يجتمع المشاركون في غرفة مجهزة بكاميرات وشاشات تعرض غرفاً مشابهة في الموقع البعيد. وقد أنتجت بعض الشركات مثل PictureTel و Intel نظام مؤتمر فيديوياً يعتمد على هذا النموذج باستخدام خطوط الهاتف النظامية، وذلك منذ عشر سنوات تقريباً، ولكن هذه الأنظمة الخاصة قد تكون محبطة من حيث ثمن إعدادها وصيانتها، كما أنها لا توفر المرونة في التعامل، ومن ثم طُبِّق النموذج السابق على الحواسيب الشخصية حيث أن استخدام بروتوكولات TCP/IP على شبكة إثرنت يقدم بيئة أفضل للتطبيقات التي تحتاج إلى نقل الصوت والصورة معاً، وهو ما يدعى بالنموذج

"المكتبي" الذي يعمل كما هو الحال في إجراء مخابرة هاتفية، الأمر الذي يسمح للمشاركين في المؤتمر بطلب المشاركين الآخرين من حواسيبهم الشخصية. أعتمد هذا النموذج في بيئة الإنترانت التي تقدم حلولاً بعرض حزمة أكبر من الحلول التي تعمل على خطوط الهاتف النظامية. وعلى النقيض من الإنترنت فإن مدير الشبكة في شبكة الإنترانت التعاونية قادر على التحكم بنمط الاتصال بين الحواسيب التي تستخدم تطبيقات المؤتمر الفيديوي، مما يجعل مستويات الفعالية أكثر قابلية للإشراف والإدارة.

هذا النوع من الاتصال بدأ بجذب الانتباه عندما أصدرت جامعة Cornell برنامج CU-SeeMe مجاناً على حواسيب الماكينتوش عام 1993، حيث سمح هذا البرنامج بالاتصال بين نقطتين، وكذلك بالاتصال بين مجموعة وذلك ببث الصوت والصورة عبر الإنترنت. ومنذ إصدار هذا البرنامج، فإن أكثر من نصف مليون شخص قاموا باستقدام هذا التطبيق إما لإعادة إنتاجه أو للاستفادة منه في أمور تعليمية. ومن ثم أصدرت نسخ تجارية من هذا التطبيق مثل النسخة المحسنة التي أصدرتها شركة تدعى White Pine مما جعل هذا البرنامج قابلاً للتطبيق في الاتصالات في عالم الأعمال. وهناك الآن العديد من التطبيقات العاملة على شبكات الإنترانت والشبكات واسعة النطاق والتي تقدم خدمة المؤتمر الفيديوي.

ويتكون نظام المؤتمر الفيديوي من الأجزاء الأساسيّة التالية:

- صورة: كاميرا، بطاقة تحصيل فيديو.
- صوت: ميكروفون، ومكبرات صوت أو سماعات.
- شاشة عرض.
- البرنامج الأساسي.
- برمجيات ترميز.

العامل الحدي في تطبيقات المؤتمر الفيديوي هو استهلاك عرض حزمة النقل، ويمكن أن نعرّف عرض الحزمة بأنه كمية المعلومات التي يمكن أن يعالجها وسط نقل معين خلال واحدة الزمن. ويستهلك نقل الصوت والصورة من خلال أي قناة اتصال كمية كبيرة من عرض الحزمة. ولتجنب الاختناقات في

الشبكة يجب أن نأخذ بعين الاعتبار الأمور المطروحة في الفقرات التالية والتي تتعلق بمعايير الضغط ومتطلبات المخدّمات وبرمجيات الزبون.

5-4-2 مخدّمات المؤتمر الفيديوي

تستخدم تطبيقات المؤتمر الفيديوي بروتوكول UDP (User Datagram Protocol) لإرسال سلسلة من المعلومات بدلاً من إرسال طرود من المعلومات. يترك هذا البروتوكول مسؤولية التحقق من وثوقية النقل إلى التطبيق، ولذلك فإنه أكثر قدرة على إدارة التغذية بالمعلومات الديناميكية الضرورية للمؤتمر الفيديوي. كما يضمن بروتوكول UDP أفضلية نقل المعلومات الجديدة على التحقق من صحة ما جرى إرساله، فبدلاً من التحقق من وصول كل طرد، يحافظ البروتوكول على تدفق ثابت للمعلومات الجديدة. إن هذه الطريقة في العمل ضرورية لأن الطرود الضائعة من الصورة لن تسيء إلى فهم المستخدم للمعلومات المنقولة بالدرجة نفسها التي تفعلها الطرود النصية أو الصوتية. وهكذا يجب في حالة نقل الصور الحفاظ على تدفق المعلومات الجديدة، في حين تأتي أهمية حجز الموارد لتطبيقات التحقق من الأخطاء في الدرجة الثانية.

تقنية العاكس

يجعل بروتوكول UDP عملية تطوير مخدّم فيديو ممكنةً، ويُسمى هذا المخدّم بالعاكس (Reflector). وظيفة هذا المخدّم هي توجيه تدفق سلاسل المعلومات أثناء المؤتمر على نحو يحسّن من مقدرات عرض الحزمة، وعند ربط العديد من العواكس بعضها مع بعض في شبكة موزعة، يمكن أن نضمن قابلية التمديد ونزيد من التغطية عن طريق دعم مختلف أنواع الأجزاء الشبكية. وبإمكان مدير الشبكة أن يعدّل من إعدادات المخدّم عند ازدياد عدد المستخدمين من أجل ملاءمة شبكة تستخدم العديد من البنى المادية المختلفة. وتستطيع العواكس أيضاً أن تعمل كعناصر فعالة لإدارة عرض حزمة النقل كما سنرى لاحقاً.

المؤتمر الفيديوي بدون عواكس

لفهم دور العاكس في تسهيل المؤتمر الفيديوي عبر الإنترنت من المفيد مناقشة كيفية عقد المؤتمر الفيديوي بين مجموعة ما بدون استخدام العاكس. تستخدم بعض المنتجات طريقة البث الوحيد الاتجاه (Unicast Method)، حيث تنقل سلاسل المعطيات المستقلة إلى كل مشترك على التتالي، ويكون عرض الحزمة المخصص لكل مشارك في المؤتمر معداً بصورة مستقلة عن الآخرين. تستهلك هذه الطريقة عرضَ حزمةِ نقلٍ مفرطاً بسبب إرسال نسخ متعددة من سلاسل معطيات الصوت والصورة لكل مشارك في المؤتمر.

هناك منتجات بديلة تستخدم الإمكانيات MBONE (Internet Multicast Backbone) المصممة لتقنيات البث المتعدد. يتطلب البث المتعدد نقل المعلومات من حاسوب معين إلى مجموعة من الحواسيب التي قد لا تكون على الشبكة نفسها. ولقد بدأت المؤتمرات المبنية على أساس تقنية MBONE في أواخر الثمانينيات، وفي عام 1994 كبر النظام ليشمل أكثر من 1,200 شبكة مستقلة، ولا يزال هذا الرقم في ازدياد متسارع. ولسوء الحظ فإن هذه المنتجات تنقصها بعض المزايا الجوهرية، فهي على سبيل المثال لا تنقل المعطيات إلاّ عندما يراقبها المستخدم فقط، فنحن إذا أردنا التقليل من استهلاك عرض حزمة النقل فلن نرغب بأن يعمل المؤتمر الفيديوي عندما لا يراه أحد. إضافةً إلى أن هذه المنتجات تتطلب نوعاً مخصصاً من الموجّهات والبرمجيات المهيأة للاستفادة من البث المتعدد. ولتهيئة موجه MBONE (mrouter) يجب بذل جهدٍ كبيرٍ على الرغم من أنه يتطلب صيانة يومية قليلة نسبياً.

مثال

برمجيات العاكس CU-SeeMe مكتوبة بلغة C ويمكن ترجمتها وتثبيتها على العديد من بيئات UNIX بما فيها Solaris، SGI، BSD، FreeBSD، OSF-1. كما أن هذا البرنامج متوفر للعمل على بيئة Windows NT و Windows 95.

يمكن تهيئة العاكس بسرعة للعمل على نمط البث الوحيد (Unicast mode) الذي يسمح بالاتصال من نقطة إلى نقطة، أمّا لإعداده للعمل على نمط البث المتعدد (Multicast) فيجب توفر الوقت والخبرة.

5-4-3 عرض الحزمة وضغط الصورة

بالنسبة لمديري النظام، فإن المعضلة الأساسية في إضافة خدمة المؤتمر الفيديوي إلى الإنترانت هي في التوفيق بين السرعة ونوعية الصوت والصورة من جهة ومتطلبات عرض حزمة النقل من جهة أخرى. وعلى الرغم من صعوبة قياس مقدار عرض الحزمة الضروري لبث الصوت والصورة عبر الإنترنت، فمما لاشك فيه أن عرض الحزمة المطلوب كبير جداً. وللتقليل من قيود عرض الحزمة لابد من زيادة هذا العرض بإجراء تغيير في أوساط النقل المستخدمة أو تحسين طرق الترميز والضغط.

ولزيادة عرض حزمة النقل يمكن استخدام قنوات اتصال ذات عرض حزمة نقل كبيرة مثل ISDN إثرنت، أو إثرنت السريعة (Fast Ethernet)، أو ATM والتي تعتبر مثالية لتطبيقات المؤتمر الفيديوي.

أمّا بالنسبة لبرمجيات الضغط والترميز المستخدمة، فإن المنهجية التي تعمل بها خوارزميات الضغط المختارة يجب أن تكون مستقلة نوعاً ما عن بنية الإنترنت التحتية. ومن الضروري فهم آلية عمل هذه الخوارزميات في ضغط المعطيات، وكيفية التعاون مع المنتجات البرمجية الأخرى، وسلوكها في حالة شبكات ذات حمل نقل كبير.

يستخدم العديد من المنتجات المتوفرة اليوم معايير H.261 لضغط الفيديو، وعندما تعمل مع خوارزميات ضغط الصوت المعيارية فإن العنصرين يشكلان معيار H.320. صممت هذه المعايير أصلاً من أجل المؤتمر الفيديوي عبر الهاتف، وتدعم هذه المعايير نوعين من حجوم الإطار:

- معيار QCIF: حجم الإطار 176×144 Pixel.
- معيار CIF: يعطي حجماً أكبر من 352×288 Pixel.

نلاحظ أن كلا الحجمين لا يصل إلى حجم الشاشة.

يتغير عدد الصور في الثانية، والمسمى بمعدل نقل الأطر (Frame Rate)، حسب سرعة وعرض حزمة وحدة المعالجة المركزية CPU. إذا كان لدينا على سبيل المثال عرض حزمة نقل للفيديو بمقدار 128KBps وعرض حزمة نقل للصوت بمقدار 64KBps، فإن هذا يمكن أن يؤدي إلى معدل نقل بمقدار خمسة إطارات في الثانية، وهذا المعدل كافٍ للمؤتمر الفيديوي، ولكنه لا يكافئ معدل نقل الصوت بنوعية VCR الذي يساوي 30 إطاراً لكل عرض حزمة. ويمكن تفسير ذلك بأن الصوت يُنقل على الإنترنت ضمن إطارات، وفي حالة المؤتمر الفيديوي يجب أن تتوافق إطارات الصوت مع المعطيات الفيديوية. وفي كل الأحوال هناك تأخير ينتج عادةً عن ضياع الطرود الصوتية، الأمر الذي يؤدي إلى إشكالية أكبر من تلك التي تمليها ضرورة التخلي عن النوعية الجيدة في نقل الفيديو للحفاظ على نوعية الصوت.

يمكن إهمال إشكاليات عرض الحزمة في المؤتمر الفيديوي على الإنترنت حيث أن الكثير من الأدوات التي تدعم تطبيقات المؤتمر الفيديوي تعطي حلولاً مقبولة، فالعواكس تستطيع أن تعمل كمدير فعّال لعرض الحزمة. على سبيل المثال تستطيع المخدّمات من شركة White Pine أن تزيد معدّل البث للمستخدمين الأفراد حتى في أثناء حركة النقل الشديدة على الشبكة. كما تستطيع العواكس إدارة المعطيات لدعم تطبيقات أخرى مثل WhiteBoards أو نوافذ المحادثة. ومن الأمور المهمة في العواكس أنه يمكن تحديد معدل نقل أصغري تمكن زيادته ليتوافق مع مختلف سرعات الوصلات في الشبكة. من ثم يمكن تهيئة عرض الحزمة للأداء الأمثل من أجل أجزاء الشبكة المبينة على أساس ISDN أو ATM أو خطوط الموديم. وبالنسبة لمزودي خدمة الإنترانت فإن مقدرات العواكس في إدارة عرض الحزمة ضرورية، حيث يجب عليهم الموازنة بين متطلبات شبكاتهم التي لا تدعم المؤتمر الفيديوي وبين عرض الحزمة التي يستهلكها مستخدمو المؤتمر الفيديوي خلال أوقات متفرقة من اليوم.

أخيراً يجب على مدراء النظام وضع جزء من مسؤولية إدارة عرض الحزمة على عاتق المستخدمين الأفراد أنفسهم. ومن آداب استخدام المؤتمر الفيديوي تجنب استهلاك عرض حزمة النقل استهلاكاً

كبيراً، فيجب ألاّ يترك المستخدمون نوافذ المؤتمر الفيديوي تبث غرف المكتب الفارغة، ويجب أيضاً تذكير المستخدمين بضرورة الاقتصاد في عرض حزمة النقل وذلك بتجنب الاتصالات غير الضرورية.

5-4-4 برمجيات وتجهيزات المستخدمين

هناك العديد من المجموعات البرمجية والتجهيزات الضرورية لتحقيق المؤتمر الفيديوي على الإنترنت وهي متوفرة من شركات مثل White Pine، Automated Management Systems، Connetix، Insoft (Netscape)، BBN Systems and Technologies. يلخص الجدول (5-4) هذه المنتجات:

المنتج	UNIX	PC	Mac	الشركة	الموقع على الإنترنت	ملاحظات
CU-SeeMe		*	*	White Pine	www.cu-seeme.com	
CoolView [1]		*		Netscape (Insoft)	www.home.netscape.com or www.insoft.com	
Picture-Window	*			BBN	www.bbn.com	
CineVideo		*		Cinecom	www.cinecom.com	
FreeVue		*		N/A	www.freevue.com	
Video Phone		*	*	VIC Hi-Tech	www.connectix.com	ليس تطبيق TCP/IP

[1] يرتبط بـ Netscape Navigator

الجدول (5-4): منتجات المؤتمر الفيديوي

وفيما يلي ميزات بعض هذه البرمجيات:

يعمل تطبيق CU-SeeMe الخاص بشركة White Pine ضمن بيئة Windows وعلى الماكينتوش، حيث يمكن فتح ثمانية نوافذ مشاركة في المؤتمر الفيديوي إضافةً إلى عدد غير محدد من نوافذ الصوت والمحادثة. يبدأ المؤتمر برسالة تنبيه عندما يطلب أحدهم عقد المؤتمر، ومن ثم تُعرض ورقة بيضاء

(whiteBoard) للتعاون أثناء المؤتمر. كما تدعم هذه الشركة مستعرض Mosaic لتشغيل البرنامج مباشرة من موقعها علي الوب، وتسمح كذلك باختيار خوارزميات الضغط الصوتي، حيث يمكن اختيار إعدادات زمن التقطيع من إحدى القيمتين: 100 ms أو 50 ms ؛ أي أن الترميز الصوتي يمكن أن يكون:

- 2.4KBps أو 8.5KBps لدعم وصلات موديم بسرعة 14.4KBps و28.8KBps.
- 16KBps أو 32KBps لعرض حزمة نقل أكبر.

تتوفر مزايا إضافية لدعم الألوان الحقيقية على 24bit أو ألوان بالأبيض والأسود على 4bit، وكذلك يقدم البرنامج دفتر مكالمات لحفظ وإضافة وتحرير عناوين مواقع المشتركين والعواكس، كما يمكن اختيار إعدادات ضغط الفيديو بدقة قياسية أو عالية، وكلمات للسر للتحقق من هوية الطالب، وأمور أخرى تتعلق بأمن الكالمة والمؤتمر. تثبيت البرنامج سهل ومتوافق مع برمجيات شبكات TCP/IP.

أنتجت شركة InSoft (التي تملكها Netscape حالياً) برامج CoolTalk و CoolView خصيصاً لبيئة Windows 95، وقد صممت هذه البرامج لتعمل ضمن مستعرض Netscape ولذلك لا داعي لترك المستعرض لاستخدام برنامج المؤتمر الفيديوي. ومن سيئات استخدام هذه البرامج أن كل المشاركين في المكالمة يجب أن يملكوا برمجيات هذه الشركة، ولا يبدو أن شركة Insoft تنوي أن تنتج برنامجاً مماثلاً للعمل على الماكينتوش، ولكن توجد نسخة تعمل على UNIX.

أصدرت شركة BBN Systems and Technologies تطبيق PictureWindow الذي يشكل مجموعة برمجية تسمح للحاسوب بتشغيل المؤتمر الفيديوي على شبكات IP. ويستخدم هذا البرنامج برنامج Video Pix frame-capture وكاميرا فيديو من شركة Sun ليعمل المؤتمر الفيديوي بالألوان على محطات SPARC التي تعمل بالأبيض والأسود.

وأخيراً هناك عوامل إضافية تتدخل في اختيار البرنامج المناسب بما فيها متطلبات أمن الشبكة ووثوقية دعم المنتجات ونوعية النقل، وسنقدم فيما يلي عرضاً للمتطلبات الدنيا اللازمة لتشغيل تطبيقات المؤتمر الفيديوي على بعض الأنظمة.

1- المتطلبات الدنيا في الماكينتوش

- نظام التشغيل Mac OS 7.x مع ذاكرة 8 MB (ويفضّل 16 MB).
- Connectix VideoCam أو بطاقة فيديو مع كاميرا فيديو.
- ميكروفون ومكبر صوت.

2- المتطلبات الدنيا لبيئة Windows

- حاسوب 486DX/66 مع ذاكرة 8 MB RAM.
- Connectix QuickCam مع مرقّم تسلسلي.
- ميكروفون ومكبر صوت.
- كرت صوت 8-bi (ويفضّل 16-bit)
- كرت عرض 8-bit بدقة 640-480.

ملاحظة

بعد تثبيت برنامج المؤتمر الفيديوي يجب اختباره على أحد العواكس، وعند الاتصال مع العاكس يجب أن نأخذ بعين الاعتبار أن بعض العواكس لا تسمح بمعدّل اتصال أكبر من 80KBps.

5-4-5 فوائد المؤتمر الفيديوي

بالنسبة للإنترانت فإن تطبيقات المؤتمر الفيديوي يمكن أن تستخدم لوصل مجموعات العمل المتفرقة، كما يمكن استخدامها في التعليم والتدريب من مواقع بعيدة، ولتوفير بث ترفيهي أحياناً. يتطور حالياً الاستخدام التعاوني لتطبيقات المؤتمر الفيديوي من مرحلة الاختبار بين مجموعات صغيرة وفي مشروعات تجريبية إلى وسيط نقل ثابت بين مجموعات مختارة من المستخدمين. وتبنّي تطبيقات

المؤتمر الفيديوي هو خيار قابل للتطبيق على نحو متزايد، حيث أن بعض المستعرضات التي ظهرت مؤخراً تملك مقدرات صوت وصورة.

تطور Netscape حالياً المستعرض Atlas الذي يقدم دعماً كاملاً لمحيط LiveMedia لكاملة برمجيات نقل الصوت والصورة في الزمن الحقيقي في المستعرض نفسه.

وفيما يلي بعض الأمثلة التي توضح مجالات استخدام المؤتمر الفيديوي في شركات مختلفة الاهتمامات وذلك للتقليل من كلفة السفر، وتسهيل وتسريع الاتصالات لنقل المعلومات الحساسة:

- *مجال المبيعات والتسويق:* يمكن استخدام المؤتمر الفيديوي مثلاً لتأمين الاتصال بين مكاتب المبيعات والمركز الرئيسي، مما يؤدي إلى التوفير في نفقات السفر ويعزز عملية توزيع المعلومات بين المراكز الرئيسية ومختلف أنواع مواقع العمل. يُستخدم المؤتمر الفيديوي في شركة Ameritech لتحقيق الأهداف السابقة.

- *خدمة الزبائن التقنية:* تستخدم شركة SAP AMERICA المؤتمر الفيديوي لتقديم الدعم الفوري للزبائن شخصياً، لتوفير نفقة زيارة الزبائن في الموقع.

- *إدارة السندات التجارية:* طورت شركة Chase Manhattan Bank عملية المفاوضات بين مديري السندات التجارية وحسابات المؤسسات بالاستفادة من إمكانيات المؤتمر الفيديوي.

- *مقابلة المرشحين:* في معهد Georgia Tech يقوم العاملون باستخدام المؤتمر الفيديوي لمقابلة المرشحين في الزمن الحقيقي من دون حاجة إلى السفر.

- *التطبيقات الطبية:* قامت شركة معالجة بالأشعة باستخدام المؤتمر الفيديوي للتخاطب مع اختصاصيين عن بعد، والحصول على استشاراتهم من خلال إرسال الصور الشعاعية وتسجيل العمليات الجراحية.

5-4-6 تحقيق المؤتمر الفيديوي في الإنترانت

يعتقد المتحمسون لفكرة المؤتمر الفيديوي على الإنترنت أن هذه الطريقة ستصبح الطريقة الأولى في اتصالات الأعمال، ولكن نظراً للقيود المتعلقة بالضغط وعرض حزمة النقل والتي مازالت عائقاً أمام نجاح تطبيق هذه التقنية في إنترانت الشركات التعاونية، فإن تقنية المؤتمر الفيديوي مرتبطة بتطور تقنيات زيادة عرض حزمة النقل.

5-5 التطبيقات التعاونية - أنظمة قواعد المعطيات

من أهم الأمور التي تدعم وتعزز وظيفة شبكات الإنترانت هي وصل قواعد المعطيات بها، ففي عالم الأعمال الحديث المتسارع يكون توفر المعلومات أو النقص فيها هو العامل الحاسم في ازدهار أي مؤسسة أو تراجعها في ظلّ التنافس المتزايد. وهكذا فمن الضروري أن يكون كل شخص يساعد على تحقيق أهداف المؤسسة (من الرؤساء إلى أصغر العاملين) على دراية تامة بكل ما قد يؤثر على أدائه لواجباته، مثل تعديل خصائص المنتجات ومراجعة خطط الإنتاج وقوائم الاتصال بالزبائن ومتطلبات الإمداد الداخلية.

يساعد وصل قاعدة معطيات إلى الإنترانت على زيادة فعالية العمل التعاوني في الشركات والمؤسسات، الأمر الذي سينعكس على زيادة إنتاجية الشركة.

سنعرض فيما يلي أحدث تقنيات قواعد المعطيات وأكثرها قوة، والتي تؤثر على الطريقة التي تتطور بها الإنترنت والإنترانت في الوقت الحالي، وكذلك سنناقش إمكانية تطوير قاعدة المعطيات استراتيجياً للاستفادة القصوى من هذه التقنيات الحديثة، كما سنتطرق إلى الأمور التي يجب أن تؤخذ بعين الاعتبار والتي تنظر إلى نظام قواعد المعطيات كعنصر أساسي في تكوين الإنترانت، مع بعض الأمثلة عن تجارب الشركات الحالية في دمج أنظمة قواعد المعطيات في مواقعها الخاصة على الشبكة. ولقد صممت الفقرات التالية لترشد القارئ إلى الخيار الأفضل بين الإمكانيات المتاحة في عالم قواعد

المعطيات مع عرض الجانب التسويقي الذي يعبر غالباً عن قوة المنتجات ؛ ليصبح بالإمكان الاختيار على أسس علمية بدلاً من تخمين الأفضل، وهنا يجب أن نذكر أنه بالرغم من أهمية نظام قواعد المعطيات في تسهيل المهام الموكولة إلى شبكة الإنترانت (مثل توزيع الإنتاج وجدولة المشتريات)، إلا أنه من الضروري تحديد احتياجات المؤسسة الفعلية لنظام قاعدة معطيات وإلا فقد نصل إلى خيارات تؤدي إلى حلول متدنية المستوى وغير فعّالة، أو إلى حلول عالية المستوى وفائضة عن الحاجة، وبالتالي مكلفة مادياً وتؤثر على عملية الاتصالات في المؤسسة بوضوح.

وعلى الرغم من أهمية وجود قواعد المعطيات لتتميم ميزان الموارد في الإنترانت بفعالية، فمن الضروري الحذر عند استخدام هذه التقنية على المعطيات الحساسة أو الحرجة.

5-5-1 اختيار الأدوات

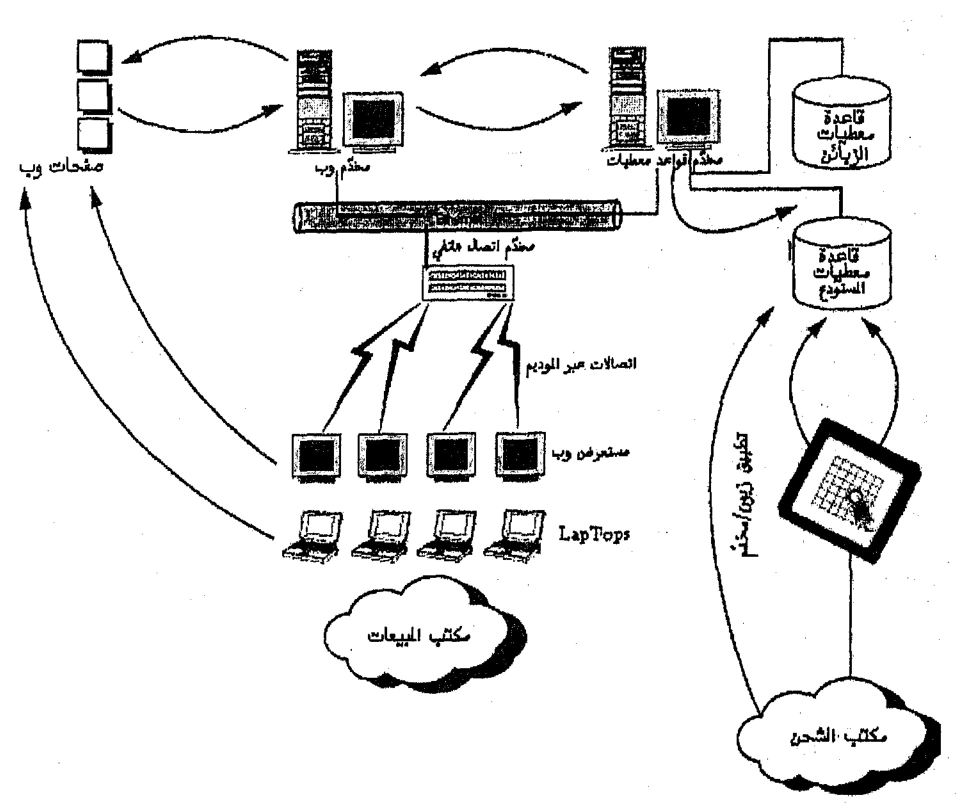
عند تقييم احتياجات المؤسسة إلى نظام قواعد معطيات (أو أكثر) ليصبح عنصراً رئيسياً في شبكة الإنترانت، يجب إدراك أن كل نظام قواعد معطيات يتألف أساساً من نظام تقليدي ولكن المزايا والخصائص المضافة إليه بهدف توسيع وظيفته قد تكون مختلفة، مما قد يؤدي في نهاية المطاف إلى وجود تباين كبير بين أنظمة قواعد المعطيات. ومن الضروري الاطّلاع على خصائص وميزات مختلف هذه الأنظمة حتى لا نجد أنفسنا أمام مشروع محكوم عليه بالفشل منذ البداية لعدم كفاية أو ملاءمة الأساس التقني.

على سبيل المثال، تصلح الأنظمة التي تقدمها شركات Informix و Sybase لعاملات الإنترانت التي تتطلب الكثير من المعالجة المعقدة، إلا أنه يمكن استخدام أنظمة أقل قدرة مثل Paradox و MS Access وتكون كافيةً لتغطية احتياجات إنترانت معينة.

إن القرار بالاعتماد على قواعد المعطيات في الإنترانت يعتبر الخطوة الأولى في عملية مهمة يمكن أن تؤثر بلا حدود على طريقة تخديم هذه الإنترانت للمتطلبات التعاونية في المؤسسات والشركات. وتوجد عموماً ثلاثة مبررات لإدخال قواعد المعطيات في تصميم شبكات الإنترانت:

1- تسمح أنظمة قواعد المعطيات بالبحث السريع والسهل ضمن مجموعة كبيرة من المعطيات لإيجاد مقاطع محددة أو معلومات ذات صلة بموضوع ما، أو مطابقة لموضوع ما. لنفترض على سبيل المثال أن أحد موظفي شركة ما يريد البحث عن طلب عرض للزبائن، أو يريد الاطّلاع على احتياجات مكتب التوريد، أو معرفة آخر التغييرات في الشركة بخصوص أحد القرارات، فإن قواعد المعطيات هي الطريقة المثلى لتصنيف هذه المعطيات، كما يمكن تضمين المميزات الخاصة مثل الكلمات المفتاحية وحقول الجداول في نظام بحث يعمل عبر الوب أو عبر خدمات الإنترانت الأخرى، يوضّح الشكل (5-7) أحد نماذج استخدام قواعد المعطيات في الإنترانت، إذ يمثل كيفية إبقاء معلومات الشركة الأساسية في متناول جميع أفراد الطاقم مع ضمان تحديث هذه المعلومات بصورة دائمة.

2- يسمح نظام قواعد المعطيات على الإنترانت بالتعديل والإضافة والحذف من عدة مواقع دون اللجوء إلى النفاذ المباشر فيزيائياً إلى الحاسوب المضيف لقاعدة المعطيات. وتتجلى أهمية هذه الإمكانية في الشركات الكبيرة التي تملك عدداً كبيراً من مكاتب المبيعات أو المكاتب الخدمية، حيث يحتاج العاملون في هذه المكاتب إلى تحديث معلومات الشركة حول المبيعات، أو إلى طلب بعض المنتجات ليُصار إلى شحنها، أو أي معطيات أخرى من شأنها أن تؤثر على الكانة التجارية للشركة. وباستخدام نظام قواعد معطيات مزوّد ببرمجيات التخاطب المناسبة يصبح بالإمكان الحصول على مثل هذه المعلومات وتعديلها بما يضمن تلبية احتياجات كل فرد من طاقم الشركة.



الشكل (5-7): أحد نماذج استخدام قواعد المعطيات في الإنترانت

وفي عالم الأعمال الذي يتطور بسرعة تزداد معها احتياجاته، يكون الحصول على المعلومة، سواء أكانت جيدة أم سيئة، في الوقت المناسب ضرورياً للغاية. فلم يعد بالإمكان التسامح مع ظهور المفاجآت بعد فوات الأوان، كم أن تمكين طاقم الشركة من النفاذ إلى السجلات الهامة من أي موقع يؤدي بالضرورة إلى تعزيز مكانة الشركة بين زبائنها.

3- المبرر الثالث لاستخدام أنظمة قواعد المعطيات هو ضرورة تقديم معطيات دورية وديناميكية للموظفين الذين يكونون على اتصال دائم مع الزبائن، فإضافةً إلى مقدرة قاعدة المعطيات على مساعدة الشركة في إبقاء معلوماتها حديثةً على الدوام، فإن نظام قواعد المعطيات يجعل هذه المعلومات في

متناول يد هؤلاء العاملين الذين يعتمدون علـى المعلومـات في اتخـاذ قـرارات هامـة. وبالاهتمـام بـهذه الحاجة فإن مسار كامل العملية التعاونية سيصبح أكثر وثوقية وسلاسة، لأن المعطيات متوفرة وحديثة على الدوام والنفاذ إليها سهل.

وإن كنّا لم نذكر حتى الآن الهدف الخاص الذي قـد تسعى المؤسسـة التعاونيـة لتحقيقـه مـن خـلال قاعدة المعطيات، فهذا لا يعني أنه ليس منسجماً مع ما عُرض حتى الآن، حيث أن تطبيقات قواعـد المعطيات تسيطر سيطرةً كبيرة في شبكات الإنترانت الحديثة.

على النقيض من بعض التقنيات والخدمات الناشئة التي أدى إليها تطويـر شـبكات الإنـترانت، فـإن أنظمة قواعد المعطيات ظهرت قبل ذلك بكثير، بحيث أصبح هناك الكثـير مـن المعلومـات المتاحـة في المنشورات والمطبوعات، إضافةً إلى العديد من مواقع الوب التي تعرض التطورات الأخيرة والتعديـلات أو معلومات التثبيت. وعلى الرغم من أننا سنعرض بعـض الأنظمـة المعروفـة جيـداً والأكـثر شـعبية في تطوير شبكات الإنترانت اليوم، إلا أنه يجب تخصيص الوقت الكافي لدراستها والبحث في الخيـارات المختلفة التي تقدمها، والتي يمكن أن تكون قد ظهرت بعـد نشـر هـذا الكتـاب وذلـك لتحديـد نظـام قواعد المعطيـات الـذي يلـبي احتياجـات المؤسسـة الخاصـة. ويجـب دائمـاً أخـذ المبـادرة مـن أجـل استكشاف التطبيقات الجديدة داخل الإنترانت بخصوص تقنيـات قواعـد المعطيـات المُدخلـة وضمـان تمديد حدود التصميم من وقت لآخر.

بما أن أنظمة قواعد المعطيات الحالية حافلة بالمزايا ومحدّدة الوظائف فإننا نحتاج إلى دراسة دور كـل ميزة على حدة في التطويـر ؛ فالخيـار الأول الـذي يتبعـه أغلـب المصممـين هـو الـتركيز علـى قـاعدة معطيات واحدة تكون موثوقة، لنقل مثلاً نظام Borland Paradox for Windows، ويبقـى الـتركيز منصباً على هذا النظام خلال دورة حياة مواقع الإنـترانت الداخليـة. ويمكـن تفـهم القيـام بمثـل هـذا الخيار، لكن المضي في هذا الطريق قد يسبب الكثير من المشاكل، ليس بالنسبة للمستخدمين (العاملين في الشركة) وإنما للأشخاص (الزبائن) الذين يعتمدون على العاملين في الحصول على معلومات دوريـة ودقيقة وفورية نوعاً ما. وإذا أخذنا جملة العوامل المؤثرة في بناء الشبكة (مثل عدد المستخدمين الذيـن

يستخدمون النظام، أو نوع وكمية المعلومات الضمنة في قاعدة المعطيات، أو تركيبة البنية المادية والبرمجية التي يعمل عليها النظام، أو أي نوع من العوامل الأخرى)، فإن نظام قواعد المعطيات المختار في الإنترانت قد يكون العامل المحدد لنجاح أو فشل تجربة الإنترانت التعاونية. فقد تفرض مثلاً احتياجات شبكة الإنترانت وجود مزيج غير متجانس من الأدوات ومصادر قواعد المعطيات لضمان بناء مواقع الشبكة بنجاح. ونحتاج مثلاً إلى مخدّم SQL للقيام بالمهمات الأولية، وبعض تطبيقات الزبون العاملة على الوب لتأمين النفاذ العام، وإلى تطبيقات زبون تعمل على حاسوب شخصي مثلاً للإشراف على النظام وإدارته أو صيانته، ....

كما أنه من الضروري تحديد دور قاعدة المعطيات قبل اختيار النظام المحدد، ولذلك يجب التريث في توقع نماذج الاستخدام واحتياجات المستخدمين قبل تبني أي تقنية.

في الفقرات القليلة القادمة سنغطي المصادر الأساسية لأنظمة قواعد المعطيات والتي يمكن اعتمادها في شبكات الإنترانت، كما سنناقش بعض القضايا المتقدمة الواجب أخذها بعين الاعتبار عند تأمين النفاذ إلى المعطيات من خلال الوب أو شبكة الإنترانت.

2-5-5 تقييم خيارات أنظمة قواعد المعطيات

يمكن تصنيف الأنظمة المتوفرة والأكثر شعبية في ثلاثة أنواع: الأنظمة العالية المستوى (Informix, Sybase, Oracle, MS SQL Server)، والأنظمة متوسطة المستوى (Paradox, MS Access)، والأنظمة البدائية (الملفات النصية). وفيما يلي بعض الأمثلة المختارة منها:

آ- الأنظمة العالية المستوى

Informix -1

تدور استراتيجية هذه الشركة حول نظام إدارة قواعد معطيات غرضي التوجه (Object Oriented Database Management System <OODBMS>) مرفق بلغة برمجة، حيث قامت بإعادة كتابة

كامل المحرك الأساسي في بداية عام 1991 ؛ وتبع ذلك شراؤها لشركة Illustra، وهي شركة متخصصة في نمذجة وإدارة المعطيات المعقدة. وقد أنتجت Informix أنظمة RDBMS (Remote DataBase Management Systems)، ونقلتُها الأخيرة قد تؤدي إلى احتلالها لمواقع أفضل في المنافسة.

وستشكل تقنيات Illustra جزءاً أساسياً من وظائف Informix الجديدة على الإنترانت، وبالتحديد فإن Illustra تدعم تضمين الأغراض المعقدة مثل الفيديو والصوت والصور، وهي أجزاء حرجة في تحديد قوة الإنترانت. وتخطط شركة Informix إلى توسيع البنية القابلة للتمديد ديناميكياً DSA (Dynamic Scalable Architecture) لمحركها، وتسعى إلى دمجه مع بنية Illustra الموسعة غرضياً. إن المحرك المزوّد بـ DSA متخصص في المعالجة التفرعية، مما يعني فاعليةً جيدةً في معالجة حمل المعلومات المتزايد، حيث يخلق نظام قاعدة المعطيات عدداً من المهمات الجزئية (Threads)، ويوزعها على عدة معالجات للمحافظة على مستوى ثابت في الأداء، وتحدد هذه الميزة مدى قابلية قاعدة المعطيات للتوسيع. تختص Informix بالجانب العلائقي (العلاقاتي) (Relational) لأنظمة ORDBMS بينما تعطي Illustra الجانب الغرضي.

ويمتلك مخدّم Informix و Illustra المسمى Universal Server القدرة على استخدام الـ DataBlades، حيث توسّع هذه الأخيرة وظيفة قاعدة المعطيات من خلال تقديمها لواجهة برمجة غرضية التوجه. وعلى سبيل المثال فإن Web DataBlade يسمح ببناء صفحات HTML تستطيع التخاطب مع المخدّم Universal Server.

ولمزيد من المعلومات عن استراتيجية Informix في شبكات الإنترانت يمكن زيارة الموقع www.informix.com.

Sybase -2

تدور عائلة تطبيقات الإنترانت في أنظمة قواعد المعطيات المقدمة من شركة Sybase حول المجموعة البرمجية لنظامها System 11، وعند استخدام هذه المجموعة مع تقنيات الإنترانت الأخرى يمكن تقديم مصادر قوية للاتصالات التعاونية. وقد قطعت Sybase أشواطاً بعيدة في التأكد من أن النظام System 11 يستطيع معالجة المعطيات التي تتطلب الدقة على الإنترانت، وفي نفس الوقت الحفاظ على درجة عالية من قابلية التوسيع والفاعلية الضروريتين لتحقيق التشارك في المعلومات. يضم النظام System 11 كل عائلة قواعد المعطيات من Sybase بما فيها SQL Server 11، Sybase IQ، Sybase MPP، وتعود شهرة Sybase إلى بنية نواة محرك قواعد المعطيات الذي يدعم تعدد المهمات الجزئية (Multithreaded). كما أن محركها متناظر تماماً وقادر على المعالجة والتحكم بالذاكرة وأمور الدخل والخرج، إضافةً إلى العديد من الأمور الأخرى التي كانت تؤدي إلى حدوث اختناقات في الأنظمة التقليدية، الأمر الذي يؤدي إلى نظام قاعدة معطيات عالي الأداء وقليل المشاكل. وعلى النقيض من الأنظمة الأخرى التي تحتاج إلى تركيبة محددة جداً من البنية المادية والبرمجية للوصول إلى الأداء الأمثل، فإن SQL Server 11 يعمل جيداً ضمن أي وسط مادي أو برمجي وبتراكيب مختلفة تتراوح من نظام بمعالج وحيد وذاكرة 12MB إلى نظام عالي المستوى SMP بذاكرة 12GB، الأمر الذي يعطي مرونة كبيرة عند دمج System 11 مع أي نظام آخر، إضافةً إلى السماح بالعديد من الخيارات لاحتمالات التوسيع المستقبلية.

طُوِّر مخدّم SQL 11 ـ العنصر الأساسي في النظام ـ للأداء الأمثل عند التشارك على المعطيات بين عدد كبير من المستخدمين المتنافسين، وتفيد هذه الميزة في بناء شبكات إنترانت في بيئة كثيرة المستخدمين.

ووجود عدة مستخدمين يحاولون الوصول إلى نفس المنطقة في قاعدة المعطيات وفي نفس اللحظة يشكل ضغطاً كبيراً على أداء النظام، مما يؤدي إلى البطء في النفاذ إلى المعلومات. وقد قامت شركة Sybase بتحليل البنية المادية والبرمجية، وعوامل الاستخدامية لتحديد الطريقة الفعّالة في التعامل مع هذه المشكلة، وبالنتيجة فإن مخدّم SQL 11 هو نظام RDBMS قابل للتوسيع ويستطيع استغلال أي

ميزة في النظام الذي يعمل عليه، ابتداءً من وحدة المعالجة المركزية والذاكرة إلى الموارد الصلبة الأخرى، وذلك لتخديم المعطيات بنسبة سريعة تتجاوز التوقعات.

متطلبات نظام Sybase SQL Server 11: (متوفر ضمن أوساط UNIX الكبرى)

- مخدّم Windows NT.
- ذاكرة بحجم 15MB من أجل مخدّم SQL.
- 48KB لكل مستخدم إضافي.
- مساحة على القرص الصلب 6MB لتخزين برمجيات النظام.

3– Oracle

عُرفت شركة Oracle منذ مدة طويلة بأنظمة قواعد المعطيات المتفوقة، ولقد أخذت هذه الشركة بعين الاعتبار متطلبات تخديم المعطيات في الإنترانت والإنترنت في تصميم منتجاتها الأخيرة مثل المجموعة البرمجية Oracle Universal Server التي تتألف من مجموعة متكاملة من تطبيقات المخدّم وتطبيقات الزبون وتطبيقات الإشراف على النظام. هذه المنتجات مصممة بحيث تكون جاهزة للتثبيت، ومعروف عنها أنها متوافقة مع أي استخدام تقريباً، وهذه الميزة مفيدة للمؤسسة التعاونية، بمعنى أن فريق التصميم يستطيع أن يركز على تصميم حلول عملية وقوية وكاملة المزايا لتلبية الاحتياجات الخاصة، بدلاً من تضييع الوقت الثمين على توسيع القيود المفروضة من قبل تركيبة البنية المادية والبرمجية في أنظمة المؤسسة.

صُمّمت مجموعة Universal Server للتكامل السريع والفعال بين خدمات قواعد المعطيات ومخدّم Oracle تحديداً، إضافةً إلى أن هذه المجموعة تقدم ميزة استعادة وصيانة وحماية المعطيات حتى في حالة بعض الأعطال المدمّرة.

وللحصول على المعلومات الوافية عن هذا النظام يمكن زيارة الموقع www.oracle.com.

متطلبات نظام مخدّم Oracle:

- نظام تشغيل Solaris أو MS Windows NT.
- معالج Pentium 100MHz فما فوق.
- ذاكرة 64MB.
- مساحة على القرص الصلب 2GB.
- متطلبات نظام Oracle الزبون:
- نظام تشغيل Windows 95 أو Windows NT ضمن بيئة بيانية.
- ذاكرة 16MB.
- مساحة القرص الصلب 500MB.
- أدوات الوب تتطلب مستعرض وب متوافق مع HTML 2.0 فما فوق.

3- مخدّم SQL من Microsoft

كما هو الحال مع أغلب منتجات شركة Microsoft فإن مخدّم SQL صُمّم في بعض أجزائه كتطبيق قائم بحد ذاته، ولكنه سرعان ما عُزّز ودُعّم بوظائف منتجات أخرى من شركة Microsoft (وتأمل شركة Microsoft من هذه السياسة أن تضمن ولاء واعتماد المستخدمين على منتجاتها). هذا يعني أنه بتثبيت IIS (MS-Internet Information Server) وبعض المنتجات الأخرى يصبح بالإمكان تصميم وبناء أنظمة إنترانت معقدّة بسهولة، بسبب التوافقية المتوارثة بين مجموعة تطبيقات Microsoft. ولكن إذا كنا نتعامل مع خليط من التطبيقات والخدمات والأنظمة (كما هو الحال غالباً) فليس من الضروري الاستفادة من تثبيت برمجيات Microsoft. وفي محاولات Microsoft لإقناع مديري نظم المعلومات للاتجاه نحو منتجاتها، فقد طورت هذه الشركة عدداً من المجموعات البرمجية لتسهيل استخدام أنظمة قواعد المعطيات المتوارثة في شبكات الإنترانت التي تقدم خدمة الوب باستخدام أنظمة مثل TransAccess من Microsoft و EDA/Open Database Gateway من شركة Information

Builder، وهذه الأنظمة متوافقة تماماً مع MS-SQL وتسمح باستيعاب مصادر المعلومات المتعذر الوصول إليها عند تصميم الإنترانت.

يُعتبر مخدّم MS-SQL فعّالاً في التوزيع الآني للمعلومات، كما أنه يساعد في تفاعل وتخصيص الموارد المتوفرة في المؤسسة على الإنترانت، وتتضمن استراتيجية Microsoft المسماة "الإنترنت الفعّالة" (Active Internet) دعماً للاتصالات التعاونية، وإضافةً إلى هذه الاستراتيجية فقد استثمرت هذه الشركة كمية غير قليلة من الوقت والجهود والموارد المالية في تطوير تقنيتها ActiveX، التي تشكّل خليطاً متماسكاً وفعّالاً نوعاً ما من التقنيات، حيث تسمح للمستخدم بالبناء والإشراف على المحتويات الديناميكية في الصفحات المنهلة باستخدام عدد من الكتل البرمجية واللغات البرمجية، إضافةً إلى تطبيقات Microsoft الأخرى عن طريق تضمينها مباشرةً في الصفحات المنهلة الثابتة المحتوى أو الديناميكية. وقد تبدو تقنية ActiveX مألوفة بالنسبة لعناصر الربط والتضمين الديناميكي (OLE) لأن الجزء الأعظم من عناصر ActiveX مبني على أساس التشارك في المعطيات، الأمر الذي تسهله OLE.

وللحصول على مزيد من المعلومات عن مخدّم MS-SQL وأهميته للإنترانت التعاونية يمكن زيارة الموقع /www.microsoft.com/sql.

وبما أن أنظمة قواعد المعطيات التي قمنا بتغطيتها حتى الآن قد تكون أو لا تكون في متناول بعض الشركات بسبب قيود تقنية أو مالية، فإنه يجدر بنا أن نشير إلى وجود بعض الأنظمة العملية أيضاً ولكنها متوسطة المستوى بالنسبة للأنظمة السابقة.

ب- الأنظمة متوسطة المستوى

Paradox -1

يعتبر نظام Paradox من شركة Borland متعدّد الوظائف ومفيداً وهو يحتوي على مجموعة كبيرة من أدوات نظام المعلومات. يتفوق الإصدار الأخير على الإصدارات الأولى بعدد من المزايا تهدف إلى تسهيل بناء قواعد المعطيات وإدارتها ونشر المعلومات. يجري ذلك من خلال إضافة العديد من "الخبراء"، أي من الإجراءات المؤتمتة التي جرى تطويرها لبناء جداول قاعدة المعطيات، ولتوليد التقارير ونماذج إدخال المعلومات، إضافةً إلى إجراءاتٍ لدمج البريد ونقل المعطيات من أنظمة أو موارد أخرى. يمكن أن تكون هذه الإمكانيات مساعدة إذا كانت الشركة تتعامل مع المعطيات من مصادر مختلفة أو تستخدم حالياً أنظمة قواعد معطيات مختلفة في مكاتبها، فإذا أردنا الانتقال إلى نظام واحد عند بناء الإنترانت فإن Paradox يستطيع تحويل كل أنواع قواعد المعطيات تقريباً إلى مصدر واحد للاستخدامات المستمرة، كما يدعم Paradox مختلف مجموعات تطبيقات الأعمال (بما فيها Microsoft Office و Perfect Office) وبالتالي يمكن التشارك بالمعطيات مع العديد من التطبيقات. إضافةً إلى ذلك، وبدعم من Paradox MS-Exchange/MAPI، أصبح بالإمكان توزيع بعض أو كل المعطيات عبر البريد الإلكتروني حيث يمكن اللجوء إلى هذا الخيار كحل بديل عند تعطُّل مخدّم الوب.

متطلبات نظام Paradox 7.0:

- حاسوب شخصي Intel 386DX أو أي معالج أسرع.
- نظام تشغيل windows 95 أو Windows NT 3.51.
- ذاكرة 12MB (ويفضّل 16MB) في حالة نظام Windows 95.
- مساحة متاحة من قرص صلب بحجم 13MB للتثبيت الأصغري، و30MB للتثبيت المثالي.
- سواقة أقراص مرنة أو سواقة قرص ليزري.
- شاشة عرض VGA أو أي دقة عرض أعلى.

- Mouse.

ولمزيد من المعلومات عن هذا النظام وأي تطبيق آخر من Borland بخصوص شبكات الإنترانت يمكن زيارة الموقع www.borland.com.

5-5-3 قضايا متقدمة في قواعد المعطيات على الإنترانت

سنتحدث فيما يلي عن بعض الأمور المتقدمة في إدارة نظم قواعد المعطيات الموزعة، وهي تتعلق بتقنيات تقسيم المعطيات ونسخها عبر مختلف المواقع، ولا تعتبر هذه التقنيات من الاهتمامات الأولى في الإنترانت الصغيرة أو متوسطة الحجم، ولكن عندما تكبر الإنترانت فقد تظهر الحاجة لإدارة قواعد المعطيات في المؤسسة. وتخفف تقنيات التقسيم والنسخ من مشاكل نمو حجم الإنترانت، حيث تشكل مسألة فعالية المعطيات محوراً أساسياً في عالم المعلومات، ومن المسائل المطروحة دائماً: أين يجب تخزين المعطيات وكيف يجب أن ننمذج العلاقة بين المستخدم والمعطيات، والحل الطبيعي هو أن تكون المعطيات قريبة قدر الإمكان من المصدر ومن المستخدم الذي يحتاجها، وفي شبكات الإنترانت، وبما أن المواقع قد تكون متباعدة، فإن الحل المتبع غالباً هو تقنيات التقسيم والنسخ.

تقنية التقسيم

هناك عدة أشكال للتقسيم؛ فتقسيم المعطيات يعني نشرها على أكثر من مصدر، حيث يمكن للمعطيات أن تكون موزعة على أكثر من وحدة تخزين، كما يمكن وجود عدة معالجات يعمل كل منها على القسم الخاص به، وهناك العديد من تقنيات التقسيم (مثل Round-Robin، Hash-Partitioning، Range-Partitioning)، كما أن التقسيم في قاعدة المعطيات يمكن أن يكون أفقياً أو عمودياً وذلك على مستوى الجدول الواحد. يجري تقسيم الجدول في التقسيم الأفقي إلى مجموعات نحافظ في كل منها على وجود الحقول كافة في جميع الأجزاء، أما في حالة التقسيم العمودي فيجري تقسيم الجدول حسب الحقول، بحيث نخزن عدداً من الحقول في موقع وأخرى في موقع آخر، والهدف دائماً في هاتين الحالتين هو أن تكون الأجزاء موجودة بقرب أماكن استخدامها الأكبر.

يكون التقسيم عادةً على مستوى الشبكات الواسعة، حيث يكون لاختناقات الأنظمة أو الشبكات بين المواقع البعيدة تأثيرٌ سلبيٌ على أداء الإنترانت ككل. ويجب الموازنة بين ضرورة إبقاء الموارد التي تتعرض للتعديل كثيراً بالقرب من المصدر واحتياجات المستخدمين البعيدين عن المصدر إلى النفاذ إلى المعطيات دورياً. وهذا ما تقوم به التقنية الثانية، نسخ المعطيات.

نسخ المعلومات

تكمّل تقنية نسخ المعلومات التقنية السابقة في عملية توزيع المعلومات، وهي تقضي ببساطة بإنشاء عدة نسخ لتحسين سرعة الوصول كما أنها قد تفيد في مجابهة الأعطال، ومن مساوئ هذه التقنية أن كلفة تعديل عدة نسخ بدلاً من نسخة واحدة ستكون بالتأكيد أكبر، كما أنها تؤدي إلى زيادة التعقيد في التحكم في التنافس على الموارد. ويمكن أن يجري النسخ على مستوى قاعدة المعطيات كاملةً (يسمى غالباً بالـ Mirroring)، أو يمكن أن يكون على مستوى الجداول، وعلى سبيل المثال فإن شركة Microsoft أنشأت نسخاً متطابقة من مخدّمات الوب خاصتها، وذلك لمواجهة الحجم الضخم من الاتصالات المتنافسة التي تأتيها خلال اليوم الواحد، وفي الإنترانت الكبيرة الحجم قد نواجه المشكلة نفسها.

لمناقشة مشاكل هذه التقنية لنأخذ المثال التالي: نفترض أن أحد المستخدمين يرغب في الحصول على بعض المعلومات من خمسة مواقع متباعدة، وزمن الاتصال بهذه المواقع يختلف بحسب حركة النقل على الشبكة، بحيث يمكن للمستخدم أن يحصل على المعلومات من ثلاثة مواقع بسرعة بينما يجب عليه أن ينتظر ورودها من المواقع الأخرى. يمكن أن يكون أحد الحلول هو جمع معلومات هذه المواقع ليلاً وإرسالها إلى مخدّم قريب من المستخدم كل يوم، وهذا الحل يعمل جيداً إذا كان المستخدم يقبل بالاطّلاع على المعلومات مرة واحدة فقط في اليوم، وإذا كانت هناك ضرورة إلى تعديل المعطيات عدداً كبيراً من المرات. وفي العديد من أنظمة قواعد المعطيات يمكن إرسال النسخ آلياً ضمن فترات محددة، بحيث يمكن في مثالنا جعل المواقع الخمسة ترسل التعديلات كل ساعتين مثلاً. قد يحل هذا الأمر المشكلة ولكن تبقى هناك بعض الحالات التي تكون فيها هذه المدة غير كافية، ولذلك تُعاير عملية

نسخ المعطيات بحسب معدل النقل في الشبكة، ففي الشبكات غير المكتظة يمكن تصغير زمن إرسال التعديلات، وتبقى المشكلة قائمة في الشبكات المزدحمة.

أنماط استخدام المعطيات

يلخص الجدول (5-5) أنماط النفاذ إلى المعطيات الأربعة الأساسية:

نمط المعطيات	البعد عن الهدف	الحاجة للتعديل	الاستراتيجية المتبعة
نمط I	قريب (محلي)	كبيرة	تقسيم/نسخ
نمط II	بعيد	كبيرة	تقسيم/نسخ
نمط III	قريب	قليلة	التقسيم
نمط IV	بعيد	قليلة	النسخ

الجدول (5-5): استراتيجيات إدارة قواعد معطيات الإنترانت

النمط I

تتمثل المعطيات من هذا النمط بقاعدة معطيات قريبة من المستخدمين الذين يحتاجون إلى تعديلها كثيراً. في أغلب الأحيان يمكن الإبقاء على المعطيات في مكانها الحالي لأنه يمكن إهمال سرعة الشبكة عندما تكون المعطيات قريبة من المستخدم، ولكن في بعض الحالات قد نحتاج إلى النسخ. لنفترض أنه لدينا مجموعة من المستخدمين الذين يقومون بالتعديلات على مقطع صغير من قاعدة معطيات كبيرة الحجم ولكنهم يحتاجون إلى الانتظار فترةً قصيرةً لتظهر لهم المعطيات معدلة ؛ من الممكن أن يكون مخدّم قاعدة المعطيات الكبيرة الحجم بطيئاً لأنه يقوم بتخديم عدة قواعد معطيات. في هذه الحالة يمكن نسخ أجزاء قاعدة المعطيات التي تحتاجها مجموعة المستخدمين والسماح لهم بالتعامل مع هذه المعطيات على مخدّم قواعد معطيات آخر مخصص لهم. بهذه الطريقة فإن مجموعة المستخدمين

تستطيع القيام بالقراءة والكتابة في قاعدة المعطيات والحصول على النتائج بسرعة. وبالنسبة للمناقلات المدرجة في الجدول والتي تحتوي تعديلات على القاعدة، يمكن أن ترسل إلى المخدّم المركزي، ولأن هذه المجموعة من المستخدمين تتألف عادةً من المستخدمين الأساسيين فهناك احتمال صغير بوجود مواقع أخرى قد ترسل معاملات يجب إلغاؤها (تؤدي إلى Rollback).

النمط II

هذا النمط من أصعب الأنماط من حيث إيجاد نموذج مناسب لطريقة النفاذ إلى المعطيات بسبب كون المصدر بعيداً والتعديلات كثيرة، وغالباً يجب استخدام تقنية النسخ لإعطاء المستخدمين البعيدين زمن وصول مقبول، وفي الأساس يؤدي النسخ إلى المزيد من المشاكل، لكن هذا النوع من الحالات لا يترك سوى القليل من الخيارات المكنة (إلا في حالة وجود اتصالات عالية في الشبكة (ألياف زجاجية)). وهذه الحالة تشابه الحالة السابقة ماعدا في أن احتمال وجود معطيات غير متوافقة بين أيدي المستخدمين قد يزداد بسبب الوقت الأطول الذي تأخذه التعديلات في الانتقال إلى المصدر البعيد.

النمط III

هذا النمط من المعطيات هو الأسهل، حيث يكون التعامل في أكثر الأحيان مع المستخدمين الذين يرغبون بالقيام باستفسارات للقراءة فقط، وبسبب قربهم من المصدر فإن زمن الوصول يبقى مقبولاً، كما أننا سنتحاشى إلغاء العاملات (بسبب تضاربات التعديل)، ويمكن ترك المعطيات مقسمة.

النمط IV

هذا النمط مماثل للنمط السابق ماعدا في أن المستخدمين في هذه الحالة يكونون بعيدين، وأفضل استخدام لتقنية النسخ يتجلى في هذه الحالة لأن المستخدمين لا يقومون بالكثير من التعديلات، والمشكلة الوحيدة هي قيود السرعة (بسبب البعد)، والتي يمكن حلها بنسخ أجزاء المعطيات التي يحتاجها المستخدمون.

مراعاة نمو حجم الإنترانت في التصميم

عند تصميم الإنترانت، يجب أن الأخذ بعين الاعتبار مكان تخزين المعطيات، وأحد الحلول الأولية يمكن أن يكون بأخذ كل المعلومات في الشركة وتحميلها على مخدّم وب مركزي، هذا الحل قد يعمل جيداً إذا كانت المؤسسة صغيرة أو متوسطة الحجم، ولكن جهازاً واحداً قد لا يستطيع أن يحمل ذاتية العاملين إذا كان تعداد العاملين يزيد عن 50,000، أو ربما أن قسم المحاسبة في الشركة بعيد عن الموقع، ويأخذ وقتاً أطول لتحميل معطياته إلى مخدّم الوب المركزي، وهكذا تظهر الصفحات حديثة ما عدا الجزء المتعلق بالمعطيات المالية.

يُعتبر تحديد مكان تخزين المعطيات مرحلةً حرجةً في بناء قاعدة معطيات الإنترانت، ويجب على المصمم النظر إلى احتياجات العمل أولاً ومن ثم تحديد حجم المعطيات، ومدة حياتها (الوقت الذي تبقى فيه المعطيات قابلة للوصول إليها)، وتوفرها (الوقت الذي يجب فيه أن تكون المعطيات قابلة للوصول إليها)، وهذه المعادلة ليست سهلة التقدير دائماً، فإحدى النقاط الواجب اعتبارها هي ميل الإنترانت والإنترنت إلى تشجيع المستخدمين على القيام بنسخ المعطيات.

يرغب العديد من المستخدمين بنسخ المعطيات التي يجدون أنها تهمهم، ويقوم آخرون باستقدام الملفات لرؤيتها فيما بعد، وفي كلتا الحالتين فإن المعلومات تكون قد نسخت من المخدّم إلى الحاسوب المحلي، وهذا النسخ قد يكون لا بأس به عند نسخ معلومات صغيرة (مثل Device Drivers أو وصفات معينة أو حتى مواعيد أعياد الميلاد). ولكنه يكون غير مجدٍ عند نسخ معلومات ديناميكية، فوظيفة المخدّم هي إبقاء هذه المعلومات حديثة على الدوام، ولكن قيام المستخدمين بنسخها واستخدام النسخ المحلية يعرضهم لمخاطر التعامل مع معطيات قديمة. تتضح ضرورة التدريب الجيد للعاملين في الشركة من خلال المثال السابق، وقد يفشل أفضل نظام عندما لا يستطيع المستخدمون التأقلم مع البيئة الجديدة.

أخيراً إن اختيار الشركة المنتجة المناسبة (والتي يجب أن تكفل تقديم معالجة فعّالة للنسخ والتقسيم) هو خيار يجب أن نتوخى الحذر عند القيام به، حيث أن كلاً من شركات Sybase وInformix

وMicrosoft وOracle تتعهد بتعزيز خدمات منتجاتها لتلبية المتطلبات الاقتصادية. وعلى الرغم من أن شركة Sybase هي أول من قام بتحقيق تقنية نسخ ثابتة تجارياً، إلا أن Informix قد تكون أفضل للاستفادة من الخاصية غرضية التوجه للقيام بالنسخ على أساس غرضي، وتقدم Microsoft خدمة نسخ متوسطة المستوى مجانية مع المخدّم SQL. وبما أن معالجة العاملات الفورية تجري عادة عبر الوب، فإن مخدّمات الوب التي تعتمد على الملفات أو قواعد المعطيات البسيطة لن تقوم بالأداء الملائم. وغالباً ما يقوم الناس بشراء منتجات بدون تفحص جميع مزاياها لأنها غير مستخدمة في الوقت الحالي، ولكن يجب التحقق من هذه المزايا عند اختيار نظام قاعدة المعطيات الذي نرغب في استخدامه في الإنترانت.

5-5-4 أمثلة تطبيقية

بعد أن قمنا بعرض الأدوات والخيارات التي تمكّن من مكاملة قواعد المعطيات في شبكات الإنترانت، سنقوم بمناقشة بعض النماذج المتعددة والمختلفة التي يمكن اعتمادها في الشركات لتعزيز فاعلية موقع الشركة باستخدام أنظمة قواعد المعطيات. يجب أن نراقب دوماً انعكاسات التنافس على تصميم أنظمة المعلومات، لكي لا تكون البنية التحتية المتفوقة لخدمات المعلومات في الشركات الأخرى سبباً في التفوق على الإنترانت التعاونية التي نرغب في تصميمها، إضافةً إلى أنه يمكن تحصيل الأفكار الجديدة من هذا المجال، والتي قد يؤدي تطبيقها إلى تحسين الأداء.

وهناك العديد من المراجع ومصادر المعلومات حول تصميم الإنترانت، وهي متاحة على شبكة الوب العالمية؛ والعديد منها يعرض (بدرجات متفاوتة) موضوع تكامل قواعد المعطيات مع أمثلة واقعية لكيفية استخدام هذه التقنيات في الشركات العالمية، وأحد هذه المصادر متوفر على العنوان home.netscape.com/comprod/at_work/index.html، كما يمكن الحصول على معلومات قيمة حول تكنولوجيا قواعد المعطيات في الإنترانت من خلال الصفحات البيضاء "White papers".

وفيما يلي بعض التطبيقات الفعلية الممكن تحقيقها في شبكة الإنترانت باستخدام أنظمة قواعد المعطيات.

البقاء على اتصال مع العاملين ومتابعة أعمالهم

مع تنامي الشركات واتساعها (أو تقلص أعمالها) والحاجة الدائمة إلى رفع الإنتاجية وتأمين الخدمات، يجب أن يكون باستطاعة العاملين معرفة معلومات الاتصال بالزبائن صحيحةً وكاملةً، وكمثال جيد لتحقيق معلومات الاتصال من خلال نظام قواعد معطيات على الإنترانت نعرض ما طوّرته شركة AT&T.

كشركة كبيرة تشغّل عدداً كبيراً من العاملين فقد أصبح الاعتماد في AT&T على المستندات الورقية والصفحات المنهلة الثابتة كوسيلة لجمع معلومات الاتصال عبر مختلف الأقسام من تقاليد الماضي، حيث قامت هذه الشركة باستغلال التقنيات الجديدة في توفير الوقت والجهود والمصاريف المالية من خلال تحقيق نظام قواعد معطيات بواجهة HTML تسمح بالبحث السريع في كامل مجلدات الشركة على أساس اسم الموظف أو العنوان أو الوظيفة أو القسم أو أي معلومات مفتاحية أخرى، وبما أن إيجاد المعلومات في هذا النظام أصبح سهلاً فقد خفّف على نحوٍ ملحوظ من أعباء أنظمة التحديث التقليدية مثل تصفح عدد ضخم من الملفات المنهلة الثابتة المضمون لإيجاد السجل الملائم للتحديث.

وصل معلومات المستودع إلى الشبكة

في بيئة الأعمال المتشعبة اليوم، يضطر مندوب المبيعات الذي يجب أن يرضي حاجات الزبون إلى حمل المنتج معه لبيعه، فقد ظهرت هذه الفكرة إثر مكاملة الأنظمة التقنية عالية المستوى مع طاقم العمل، وبظهور أنظمة قواعد المعطيات كأجزاء متكاملة في خطة الأعمال يمكن أن نضمن أننا دائماً في الموقع الملائم للاستجابة الفورية لاحتياجات الزبون الدائمة في كل وقت وفي أي مكان.

لنأخذ شركة John Deere كمثال، فقد قامت هذه الشركة لتقوية طاقمها ببناء قاعدة معطيات للقطع المنتجة على شكل صور لمختلف القطع الميكانيكية المعروضة للبيع، وزودت كل قطعة أيضاً بمعلومات خاصة مثل أبعاد القطعة وتعليمات التجميع والتصليح وما إلى ذلك من معلومات، مكّنت قاعدة المعطيات الناتجة ممثلي البيع والشراء والخدمات من النفاذ إلى المعلومات الشاملة حول منتجات الشركة، ومرة أخرى سمح النظام بعمليات أكثر انسيابية.

المتابعة الزمنية

تتجه الشركات حالياً إلى مجالات الوب والإنترانت وتقنيات قواعد المعطيات لحل مسائل تتبع مهام العاملين وساعات العمل المطلوبة لتنفيذ كل مهمة على حدة. وحالياً تستخدم الشركات مجموعة متنوعة من الطرق لتحقيق الأهداف السابقة، مثل قياس الزمن باستخدام البطاقات المثقبة، والجداول المكتوبة بخط اليد، وجداول Excel والتقارير الهاتفية، وكل هذه الطرق تحقق المهمة الأساسية وهي تسجيل ساعات العمل ولكنها تهمل الكثير من الأمور المطلوبة من وجهة نظر قابلية النفاذ للمعطيات والمرونة والمنفعة الكلية للشركة التي تأتي قبل مهمة دفع أجور العاملين.

إن نظام المتابعة الزمنية المبني على أساس الإنترانت له العديد من الحسنات للشركات ومكاتب المحاسبة. أولاً وبما أن المعلومات مخزنة في قواعد المعطيات فإن النفاذ إليها يصبح أكثر سهولة من البحث في السجلات الورقية التي قد يعود تاريخها إلى أسابيع أو أشهر أو حتى سنوات للحصول على الملف المناسب، مما يعني أيضاً سهولة تخزين كميات كبيرة من المعطيات السابقة. ثانياً، يمكن تسجيل ساعات العمل ومتابعتها يومياً بدلاً من أن تكون مجدولة أسبوعياً أو كل أسبوعين كما هو الحال باستخدام الطرق السابقة ؛ واستخدام التقنية الجديدة يؤدي إلى مراقبة أفضل لتقدم العاملين في العمل وتتبع حالة المشاريع الحالية، ويمكن بذلك تحديد أماكن الضعف والقوة في دورة تطور العاملين بدقة أكبر.

طلب وشراء المنتجات

إن العوامل المعيقة للأعمال الناجحة ليست فقط في عدم امتلاك الموارد المناسبة الضرورية لإتمام المهمات المطلوبة مثل امتلاك الحواسيب الجيدة أو حتى المستلزمات المكتبية، حيث أن قاعدة المعطيات على الإنترانت يمكن أن تلعب دوراً حيوياً لضمان حصول العاملين على أي عنصر أو خدمة مطلوبة، وباستخدام واجهة وب يمكن للموظفين استعراض محتويات المستودع وإرسال طلباتهم ليتم إيصالها لهم، وفي حال نفاذ المواد المطلوبة يمكن الطلب من المدير لشراء المزيد وفق طرق مؤتمتة.

الفصل السادس

انعكاسات الإنترنت على الشركات

تحتاج الشركات إلى القيام بتغييرات في طريقة عملها وإدارتها حتى تتوافق مع استخدام الإنترانت، فالأساليب القديمة في العمل لن تكون مناسبةً من أجل الاستفادة من الإنترانت. لذلك فإن تحقيق الإنترانت لهدفها في تقدم وتطوير الشركة، مرهون بقدرة هذه الأخيرة على تغيير عاداتها وطريقة عملها، وبقدرتها على تحمل الأعباء الجديدة التي تفرضها هذه التقنية الجديدة.

سنتطرق في هذا الفصل إلى التغييرات الواجب مراعاتها من قبل الشركات التي تستخدم الإنترانت، والتي تتناول في أدوات العمل، وطرق الإدارة، ومناهج تدريب العاملين الجديدة. كما سنبين الانعكاسات على منهجية عمل الشركة وإدارتها، والمكاسب التي تحققها الشركة من وجود الإنترانت.

6-1 متطلبات وأعباء إضافية

لا شك أن دخول الإنترانت إلى الشركة سيؤدي إلى تغيير جدي في استراتيجياتها ومتطلباتها، فاستخدام الإنترانت يوفر أدوات جديدة للاتصال والعمل المشترك، وطرقاً وأساليبَ حديثة في التسويق وعرض المنتجات. لكن بالمقابل، توجد أعباء جديدة ينبغي على الشركة تحملها، فهذه الشبكة تحتاج

إلى مراقبة دائمة من أجل ضمان تحقيق سياسة الشركة وأهدافها، كما تحتاج إلى صيانة مستمرة لئلا يتوقف العمل. سيحتاج العاملون في الشركة أيضاً إلى دورات تأهيلية ليتمكنوا من الاستفادة الفعالة من الأدوات الجديدة، وليتعرفوا على الإمكانات الجديدة المتاحة، ومدى الفائدة التي يمكن تحقيقها.

سنتعرض في هذا القسم إلى الأعباء الجديدة المنوطة بالشركة، وهي تنقسم إلى فئتين: تأهيل العاملين في الشركة، وإدارة وصيانة الشبكة.

6-1-1 تأهيل العاملين في الشركة

يحتل تأهيل العاملين وتدريبهم على طريقة القيام بالعمل باستخدام الإنترانت مكاناً أساسياً في عملية تقييم عمل الإنترانت في الشركة. فالتحدي الأساسي الذي تواجهه الإنترانت بعد وضعها قيد الاستثمار هو قدرة العاملين على استخدامها وتحقيق الفائدة المرجوة منها. إن الإنترانت المبنية والمستثمرة جيداً، تعكس كفاءة الشركة وقدرتها على إنجاز أعمالها على النحو الأفضل، ودون الحاجة إلى أي مهام أو أعباء إضافية يقوم بها الموظفون.

يُعتبر إقناع الموظفين بأهمية الإنترانت، وتخليصهم من أساليب العمل القديمة، من أهم وظائف فريق التدريب والتأهيل أثناء عملية التدريب، والتي تهدف إلى تعليم الموظفين طريقة القيام بواجباتهم ومهامهم اليومية براحة وسهولة. تُوفّر الإنترانت المال والوقت والموارد إن استُخدِمت من قبل الأشخاص المكلفين بذلك كلٌ حسب عمله.

يجب أن يراعي فريق التدريب والتأهيل مستوى المجموعة التي يقوم بتدريبها، والمعلومات السابقة التي لديهم. فلا يجب الخوض كثيراً في تفاصيل الإنترانت، وإنما يُكتفى بالتركيز على طريقة قيام المجموعة بالعمل الموكل إليها. يختلف تدريب المجموعات حسب مهمة وخبرة كلٌ منها، فالمجموعة التي سبق لها العمل على الإنترنت لن تحتاج إلى أي شرح عن الوب وأهميته، والمجموعة التي تقوم بعمليات إدارية لن تحتاج إلى معلومات عن تكنولوجيا وبنية الإنترانت. يجب التذكر دوماً بأن مهمة التدريب هي الإجابة على السؤال: ماذا تفيد الإنترانت ؟ وليس السؤال: ما هي

الإنترانت؟، كما يجب الانتباه إلى أن جلّ اهتمام العاملين يتركز في طريقة تحسين عملهم، وليس في فهم الإنترانت.

إن مهمة التدريب مهمة مستمرة وشاقة، فإضافةً إلى ضرورة تمتع المدرب بالقدرة على شرح الأمور التقنية شرحاً سهلاً ومبسطاً وبعدة أشكال، يجب أن يتحلى بالصبر والقدرة على فهم نفسية العاملين. فعندما يريد شرح بعض الإضافات الجديدة، قد يُفاجأ بعدد حضور قليل، أو يكون البعض غير مكترث، أو بتفهّم البعض للمستجدات، في حين يعترض آخرون على كل ما يحدث، كما قد يجد البعض رافضين للتقنية الحديثة، بينما يتحمس آخرون لها لدرجة اعتقادهم أن هذا التطور سوف يغير مجرى حياتهم. يجب الانتباه إلى جميع هذه الحالات، والتعامل معها بحذر وروية، فيجب أن يقتنع المعترضون ولو بعد حين بأهمية التقنيات الجديدة، وقد يصاب المفرطون في الحماس بالإحباط لأن ما سيجدونه قد يكون أقل بكثير مما يتوقعونه، لذا يجب الانتباه إليهم وتجنيبهم مخاطر الحماس الزائد.

يجب على المنهاج أن يكون مدروساً بعناية، وأن يراعي حاجات المتدربين، وتجب مراجعة المحاضرات جيداً بحيث تكون ذات مضمون جلي تماماً، كما يجب اختيار المشرفين بعناية، والانتباه إلى أن الشخص المناسب ليس بالضرورة هو الشخص الأغزر معلومات، بل هو الشخص القادر على شرح الأفكار وإيصالها بسهولة إلى أذهان المستمعين.

سنشرح فيما يلي بعض مستويات تدريب العاملين على استخدام الإنترانت.

آ- الاتصال

إن أولى الخطوات الواجب تعليمها هي كيفية اتصال العاملين بالشبكة. وقد يبدو للبعض أن هذا الأمر بسيط وبديهي، لكنه ليس كذلك بالنسبة للكثير من العاملين الذين قد يحتاجون في بعض الأحيان إلى تعليمهم طريقة الاتصال خطوةً خطوةً.

يمكن للاتصال أن يجري بعدة طرق، فمثلاً يمكن استخدام هاتف موصول مع موديم أو ISDN أو عن طريق الإنترنت. ومن أجل كل طريقة، يمكن أن يستخدم العامل نظام تشغيل مختلف. ومن هنا تمكن ملاحظة تعقيد الأمور بالنسبة لفريق العمل الذي سيقوم بتعليم كل مجموعة (أو حتى كل عامل) طريقة القيام بالاتصال حسب الإمكانية المتوفرة لديه، كما يجب عليهم إحاطة المستخدمين علماً بالمشاكل والصعوبات التي قد تعترضهم حسب كل طريقة اتصال/نظام تشغيل. وقد يكون إعداد دليل استخدام يوضح طريقة الاتصال للعاملين فكرة جيدة، إذ يمكن لهم الرجوع إليه كلما احتاجوا ذلك.

ب- البرمجيات

من المهم جداً أن تتوفر لدى العاملين الذين سيستخدمون البرامج على الإنترانت فكرةً أساسية عن برامج مخدّم/زبون. فبالنسبة لمن سيعملون على جزء الزبون، يجب أن تتوفر لديهم معلومات عن طريقة الاتصال، والبريد الإلكتروني ومستعرضات الوب، وفي بعض الحالات معلومات عن برامج المؤتمر الفيديوي أو المؤتمرات الصوتية (Audio Conferencing). أما بالنسبة لمن سيعمل على جانب المخدّم، فيجب إخضاعه لدورات تدريبية على مختلف التطبيقات المتاحة على المخدّم. فقد يحتوي المخدّم مثلاً على ... message board, calendar مما يعني أن العاملين سيتدربون على هذه التطبيقات، كما يجب أن تتوفر لديهم معلومات عن المستعرضات.

إن معرفة على ماذا سيتدرب العاملون هو الجزء السهل في العملية، أما الجزء الصعب فهو أسلوب وطريقة الشرح. الجيد في الأمر أن واجهات الوب تتصف بالسهولة بفضل HTML والمستعرضات. من أجل معظم التطبيقات، لن يكون على العاملين بذل الكثير من الجهد من أجل تعلم طريقة الاستخدام التي تقوم على أساس استخدام الفأرة من أجل النقر على مكان معين في الشاشة للانتقال إلى ما يريدون، أي الارتباطات التشعبية. ومعظم العاملين سيألفونها سريعاً، وتبقى مشكلة بسيطة مع بعض التطبيقات الأكثر تعقيداً. من أجل هذه التطبيقات الأخيرة، يجب على فريق التدريب والتأهيل أن يضع على الإنترانت معلومات عن طريقة استخدامها، بحيث تكون هذه المعلومات متاحة لمجموع العاملين الذين سيستخدمون هذه التطبيقات، وبمثابة دليل استخدام لهم.

أخيراً، يوجد أمام فريق العمل طريقتان لا غير للتدريب على طريقة استخدام البرامج هما: إما جمعهم في مجموعة أمام أحد الأجهزة ليجربوا هذه البرامج، وإمّا ترك كل شخص على حدة ليتعلم لوحده بواسطة التجريب والخطأ (Try and Error).

ج- إبقاء العاملين على اتصال دائم

إن أحد أهداف وجود الإنترانت الأساسية ضمن الشركة هو تسهيل عمليات الاتصال، وتبادل المعلومات. وأسوأ ما يمكن أن يصيب الإنترانت من مشاكل هو عزوف المستخدمين عن استخدامها.

يجب أن يعتاد العاملون على استخدام الإنترانت كما هم معتادون على تنفيذ أعمالهم ومهامهم اليومية. فعلى سبيل المثال، عندما يحتاج العامل إلى زيارة المكتبة للاطلاع على كتاب، يجب ألاّ يترك عمله ليذهب إليها، لأن بإمكانه الحصول على ما يريد من خلال الإنترانت. وعندما يحتاج إلى معرفة عدد أيام إجازاته المتبقية، لن يضطر إلى زيارة السكرتارية، فمن خلال الإنترانت سيحصل على ما يريد. إن تغيير تلك العادات، وإحلال العادات الحديثة محلها هو مهمة تحتاج إلى زمن ودراية، فليس جميع العاملين يتمتعون بالقدرة نفسها على مواكبة التطور والتغيير.

يجب أيضاً اتباع استراتيجية طويلة الأمد من أجل التخلص من العادات القديمة في العمل، وإحلال العادات التي يفرضها وجود الإنترانت محلها. فلا ينبغي على الشركات أن تفرض على المستخدمين استخدام الإنترانت بصورة فجة، بل يجب أن تعطي الأمر وقته كاملاً. فمثلاً، إذا كان العاملون معتادين على الاطلاع على التوجيهات والقرارات الجديدة من نسخ ورقية، فمن غير الصواب أن تمتنع الشركة عن إصدار النسخ الورقية لإجبار العاملين على قراءة النسخ الإلكترونية الموجودة على الإنترانت، فالأفضل هو الاستمرار في طباعة وتوزيع النسخ الورقية، مع وضع نسخة إلكترونية على الإنترانت. وفي وقت لاحق، يمكن للشركة أن تصدر النسخة الإلكترونية في وقت أبكر من النسخ الورقية، مما يمكّن مستخدمي الإنترانت من الحصول على المعلومات الحديثة بسرعة أكبر من أولئك المتمسكين بالنسخ الورقية. وشيئاً فشيئاً، يمكن تخفيض عدد النسخ الورقية حتى تصل الشركة إلى مرحلة لا تحتاج فيها إلى إصدار سوى نسخة إلكترونية فقط. كذلك يجب دراسة طرق أخرى مماثلة

لتشجيع المستخدمين على استخدام الإنترانت في المراسلات، أو قراءة الأخبار أو حتى في بعض الأحيان عقد المؤتمرات.

يُعتبر الاهتمام بالمضمون أساسياً من أجل جلب زوار جدد، أو على الأقل الاحتفاظ بالزوار السابقين. فيجب أن يشعر العامل (أو زبون الشركة أحياناً) أن الخدمة التي يستخدمها هي خدمة مفيدة، وهو لا يهدر وقته عندما يستخدمها، أيّاً كان نوعها. إن المسألة مهمة جداً، لأنه لا مجال للتراجع، فعندما يجد المستخدمون أن خدمة الأخبار (مثلاً) لم تعد جيدة كما كانت في البداية، فإنهم سيعزفون عن استخدام هذه الخدمة، مما يعني استخداماً أقل للإنترانت، وهو أمر جدي يجب الانتباه إليه دوماً. إن الوضع المعاكس ليس له هذا التأثير السلبي، فمثلاً إن لم تكن خدمة الأخبار جيدة في البداية، ثم طرأ تحسن عليها، فهذا سيجذب العاملين (وزبائن الشركة) إلى استخدام الإنترانت، وهو الأمر المرغوب على الأغلب.

د- تنظيم العمل الجماعي

من الفوائد التي يحققها وجود الإنترانت ضمن الشركة، تنظيم عمل العاملين ضمن مشروع واحد بسهولة أكبر، وعلى نحوٍ أكثر فاعلية. لنأخذ حالة شركة تعمل على مشروع برمجي ضخم. سيتبادل العاملون الكثير من الوثائق والتقارير عن العمل، وما أنجز منه، وصفاته، و... كما ستتواجد بعد حين مجموعة كبيرة من النسخ القديمة. ويوجد ضمن كل تقرير مجموعة الكثير من المعلومات المكررة. من ناحية أخرى، تحتل مواعيد التسليم وانتهاء أجزاء المشروع أهمية خاصة، وإذا طرأ أي تعديل على جزء من الخطة الزمنية للمشروع، وجب تغيير جميع المواعيد التي بعدها، وربما تغيير مواعيد أخرى متعلقة بها. إذن ستُجري الشركة العديد من الاتصالات من أجل تغيير الخطة الزمنية عند جميع الفروع التي لها علاقة. تحل الإنترانت المشكلة بسهولة تامة، فالمعلومات المتعلقة بالمشروع، من تقارير وخطط زمنية تكون موجودة في مكان واحد، وتعديلها لن يحتاج إلا إلى الدخول إلى مكان حفظ هذه المعلومات، وتعديل ما نريد فيها. فتغيير الخطة الزمنية لن يحتاج إلاّ إلى تغيير المواعيد في مكان

واحد، ولما كان بإمكان جميع الفروع قراءة تلك المعلومة من مقرهـا أينمـا كـان، فـإن هـذه التغيـيرات ستُلاحظ بعد القيام بها.

إن تنظيم العمل بهذا الشكل يحتاج إلى تدريب العاملين على طريقة استخدام الإنـترانت والبرمجيـات اللازمة من أجل إدارة هذا العمل التشاركي علـى النحـو المطلـوب. وهـذا هـو دور مجموعـة التدريـب والتأهيل التي يجب عليها أيضاً أن توضح الفوائد الكبيرة من تنظيم العمل بـهذا الشـكل، وأن تشـرح المشاكل التي يمكن التعرض لها أثناء العمل، وكيفية حلها.

هـ- التدريب ضمن مجموعة

لما كانت الإنترانت ذات طبيعة تشاركية غنية، وكان العامل الأساسي في نجاحها هـو شـعبيتها بـين المستخدمين، فإن التدريب ضمن مجموعات يساهم في إبراز هذه الطبيعة وإنجاحها. وهذا يعني الكثير من الحوار والأفكار المتبادلة. إذن السمة الأساسية في التدريب ضمن مجموعة هو الحوار الذي يضبطـه المشرف وفق الناظم: كيف نستفيد من الإنترانت.

من شروط نجاح عملية التدريب ضمن مجموعـة أن تكـون هـذه المجموعـة صغـيرة نسـبياً (حـوالي 10 أشخاص فقط)، وأن يتوفر جهاز لكل شخص. يسمح العدد الصغير للمشرف بأن يراقب المتدربين عـن كثب، فيستطيع معالجة مشاكلهم مبكراً، ومساعدتهم على تحقيق الهـدف مـن التدريـب. إن وجـود حاسوب لكل متدرب أمر ضروري، ففي الحالات التي يشـترك فيـها متدربـان علـى نفـس الجـهاز، يُلاحظ أن المتدرب الذي يملك معلومات أكثر عن الموضـوع هـو الـذي يسـتحوذ علـى الجـهاز، ويقـوم بكامل العمل، فيما يقف المتدرب الثاني متفرجاً. وإذا أراد المتدرب صاحب المعلومات الأقـل أن يقـوم ببعض العمل، فلن يتمكن من ذلك لأنه يشعر طوال الوقت بأنه مراقب وغير كفء.

من الضروري أن يشرح المشرف بعض الأمور على شاشة الحاسوب، وأن يقـوم بتنفيـذ بعـض الأعمـال بنفسه، مع شرح طريقة القيام بها. فنقطة البداية هي النقطة الأصعب في عملية التعلم، وقد لا يتمكـن المستخدم من استخدام برنامج إلا بعد جهد رغم أنه قد يكون قد قرأ كتابـاً كـاملاً حـول الموضـوع. إن

تعليم المتدربين المبادئ الأساسية الأولى يعطيهم دفعاً كبيراً وسريعاً أثناء تعلمهم على البرنامج. ويجب أيضاً أن تكون عملية التدريب والتجارب العملية ممتعة للمتدربين، وأن تعكس آفاق الإنترانت التي يمكن أن تفيد المتدربين، فيمكن مثلاً شرح برنامج دليل الهواتف وكيفية إدخال المعلومات فيه بأن يطلب من المتدربين أن يُدخل كل منهم اسمه، ورقم هاتفه، ومعلومات أخرى ضرورية مثل تاريخ ميلاده أو... يشعر المتدربون بهذه الطريقة بقربهم من الإنترانت وهي خطوة هامة نحو تعلم التقنية الجديدة.

من المفروض أن يحتوي منهاج التدريب مشروعاً بسيطاً ينفذه المتدربون بأنفسهم، وينبغي أن يُراعى فيه تطبيق ما تعلموه من أساليب العمل الجماعي، كأن يوزع المشرف مهام الشركة عليهم جميعاً، بحيث يمثل كل شخص منهم فرعاً من فروع الشركة، ويطلب منهم القيام بأحد أعمال الشركة التي تتطلب تعاوناً بين عدة فروع. ينبغي طبعاً التركيز في هذه المشاريع على الفائدة والمبادئ، وليس على النتيجة.

إن تأمين مستلزمات عملية التدريب أمرٌ يجب الإعداد له قبل البدء بأي تدريب، فلا معنى لدورة تدريبية على الإنترانت دون وجودها مع الكثير من المعلومات والتطبيقات عليها. فظهور الإنترانت كمكان يعج بالمعلومات والزوار، أي كوسط تخاطبي غني، أمر مهم جداً، وإنترانت بدون معلومات وزوار تترك أثراً سيئاً عند المستخدمين الذين قد لا يستخدمونها بعد انتهاء الدورة التدريبية!.

و- التدريب عبر الإنترانت

تحدثنا فيما سبق عن عملية التدريب على استخدام الإنترانت، لكن عمليات التدريب كانت تجري في أماكن مخصصة لهذا الغرض. إن الاستخدام الأكثر تطوراً هو استخدام الإنترانت نفسها من أجل تعليم العاملين على طريقة استخدام بعض الأدوات. لا نتحدث هنا عن ملفات تشرح الأداة وتوضع على على الإنترانت، بل نتحدث عن طريقة تخاطبية للتعليم، كما سيتضح فيما يلي.

يمكن استخدام الكثير من الأدوات على الإنترانت في التعليم، فيمكن مثلاً استخدام Message Board في تلقي الأسئلة، وإعطاء الأجوبة على أسئلة المستخدمين التقنية. فبإمكان شركة تُطوّر منتجاً جديداً أن تتيح Message Board للزوار من أجل طرح أسئلة عن المنتج: ما هو، كيف يعمل، كيف نستفيد منه... في الحالات التي تتيح فيها الإنترانت خدمة مؤتمرات الفيديو، يمكن للمشرف أن يشرح ما يريد شرحاً حياً، كما لو كان الشخص المتدرب معه في نفس المكان،لأن بمقدور كلٍ منهما أن يرى الآخر على شاشة الحاسوب.

يمكن للمشرف أن يستخدم الإنترانت في عرض محاضرته (Presentation) عن طريق برنامج ما، فبدلاً من عرض الشفافيات، التي تحوي صوراً عن طريقة عمل البرنامج، على جهاز الإسقاط (جهاز عرض الشفافيات)، يمكن عرض هذه الصور على شاشة الحاسوب من أجل توضيح مراحل عمل البرنامج المختلفة. يمكن شرح هذه الصور بكلام مكتوب على جانب الصورة، وفي الحالات التي تُزوّد فيها الإنترانت بمخدم RealAudio، يمكن أن يُسجل المشرف الشرح كملف صوت، وبنقرة من الفأرة على الصورة المعنية، يمكن أن يسمع المتدرب شرحاً عن هذه الصورة.

ز- تجارب الشركات في تأهيل العاملين

بعد أن شرحنا مهام وإمكانات التعليم من أجل تدريب العاملين ضمن الشركة على استخدام الإنترانت، سنتناول الآن بإيجاز عملية التعليم في إحدى الشركات التي كان لها تجربة مع هذه التقنية الجديدة. إن شرح تجربة هذه الشركة يفيد في إغناء ما تحدثنا عنه، وقد يفيد في وضع لمسة من الواقعية على ما سبق، لئلا يظهر كنوع من التنظير والبعيد عن الواقع.

شركة (SGAA) *The Sporting Goods and Apparel Association*

لهذه الشركة نوعان من المستخدمين الذين يريدون الاتصال بها هما: العاملون في الشركة، والأعضاء (الفروع والشركاء). كان تأمين عملية اتصال العاملين أمراً يسيراً لأنهم كانوا ضمن نطاق الشبكة المحلية LAN، وكل ما فعلته الشركة هو تنصيب البروتوكول TCP/IP ومستعرض Internet

Explorer على حواسيبهم، لكن الأمر كان أكـثر تعقيداً مـع الأعضـاء. يتصـل جميـع الأعضـاء عـبر الإنترنت، لذا كان على الشركة أن تنشر تعليمات عن طريقة الاتصال باستخدام الإنترنت. لكـن رغـم ذلك، عانت الشركة من وجود بعض الأعضاء الذين لم يستطيعوا إعداد حواسيبهم من أجـل الوصـول إلى مزود إنترنت (ISP). وقد عثرت الشركة على مزود إنترنت متواجـد في المنطقـة الـتي يوجـد فيـها أعضاؤها، وبالتعـاون معـه، نشـرت كتابـاً عـن طريقـة الاتصـال بمـزود الإنـترنت، وكيفيـة الاتصـال بالشركة، وبهذا حلت المشكلة الأولى في عملية التدريب.

سعت الشركة لأن يعتاد المستخدمون علـى التقنيـات الجديـدة، وأن يسـتخدموا الإنـترانت بـدلاً عـن الوسائل التقليدية، وقد اتبعت خطةً على مراحل وخلال فترة زمنية بلغت ثلاثة أشهر. وقــد اهتمـت خصوصاً بأن تكون الشبكة كاملة التجهيز عند موعد الافتتاح، فاختبرتها جيداً قبـل الموعـد المحـدد. فيما يلي المراحل التي اتبعتها الشركة:

المرحلة الأولى: لمدة شهر واحد. دعت ثلاثين شخصاً لاختبـار الموقـع، وإمكانـات التجـول، وأدوات الاتصال. وقد اختبروا جيداً الأدوات والخدمات المختلفة مثل:

Audio-Conferencing Functions, Message Boards, Interactive Scheduling, Contract Database, Chat, ...

المرحلة الثانية: لمدة شهر واحد. سُمح للمستخدمين باسـتخدام الإنـترانت، وراقـب الفريـق المسـؤول عمل الشبكة، ومدى رضى الناس عن المعلومات التي كـانوا يجدونـها كـل يـوم. وبـدلاً مـن فاكسـات الأخبار العشرة التي كانت ترسلها الشركة أسبوعياً إلى كلٍ من أعضائها، صار الأعضاء يتلقون صفحـة واحدة فقط تحوي ارتباطات تشعبية إلى الأخبار على الموقع. الأخبار على الموقع كانت أكثر تفصيـلاً، بينما الصفحة المرسلة إلى الأعضاء (كما ذكرنا) لم تكن تحوي سوى ارتباطات تشعبية إلى هذه الأخبار. راقب فريق العمل مجموعة الأشـخاص الذيـن كـانوا يدخلـون إلى الأخبـار، وأولئـك الذيـن لم يكونـوا يقومون بذلك.

المرحلة الثالثة: لمدة شهر واحد. تابع فريق العمل بإضافة المعلومات إلى الموقع، وأصبح بإمكان المستخدمين الحصول على أحدث الأخبار فوراً. أمّا الأعضاء الذين لم يدخلوا إلى الأخبار على الإنترانت، فقد استمرت الشركة بإرسال فاكسات الأخبار إليهم كل أسبوع.

بسبب قدرة الإنترانت الخاصة بالشركة على التواصل والتخاطب، فقد تغيرت طريقة تعامل الشركة مع أعضائها عبر الزمن. فأصبحت الشركة تصدر الأخبار فوراً، ودون الحاجة إلى استخدام الفاكسات. كما أصبح بإمكان المستخدمين أن يضعوا الأخبار التي تتعلق بهم، وبهذا يمكن لأي شخص مهتم أن يصل إليها من خلال إنترانت الشركة.

كما تزايدت فرص اللقاء بين الأعضاء، ففي السابق، كانت الاجتماعات بينهم سنوية، أو عن طريق ترتيب لقاء خاص. أما الآن، فيمكن للأعضاء الاتصال فيما بينهم في أي وقت كان، باستخدام Message Board، أو أن يجددوا عقودهم من خلال Contract Database، أو حضور اجتماعات تجري على الإنترانت. كذلك تحسنت إنتاجية العاملين، فأصبح بإمكانهم استثمار الوقت الذي كانوا يصرفونه على الاتصالات في إعداد أخبار جديدة، وتوفيرها للزوار.

جرت عملية التدريب في مجموعات خلال المؤتمر السنوي، وذلك بسبب البعد الجغرافي الكبير مع الأعضاء. وقد دُعي مستخدمون للإنترانت من مختلف الشركات الأعضاء لحضور المؤتمر ولاتباع الدورة التدريبية. لكن بسبب الكلفة الباهظة التي يتطلبها توفير حاسوب لكل شخص، والكلفة العالية للاتصالات المطلوبة عبر الإنترنت، فقد استعاضت الشركة عن الشرح على الحاسوب، بأن أقامت محاضرات عن طرق الاستخدام، مدعومة بصور لتوضيح طريقة الاستخدام. طبعاً لم تكن النتائج على المستوى الذي كنا سنحصل عليه فيما لو استُخدمت الحواسيب، لكن رغم ذلك، أصبحت لدى المستخدمين فكرة أوضح عن الإنترانت التي يستخدمونها، وعن الأدوات الموجودة. وقد وّزع كتيب خاص بالدورة ساعد أيضاً في توضيح الأدوات، وطريقة عملها.

تعقد الشركة كل شهر مؤتمراً فيديوياً على الإنترانت تشرح من خلاله مجموعة الأدوات الجديدة، كما تشرح بعض الأدوات الموجودة سلفاً. وبسبب الاختلاف في مستويات العاملين في الشركات الأعضاء،

تحدد كلٌ من هذه الشركات المواضيع الأكثر أهمية للعاملين فيها. ومن الطبيعي أن تكون الطلبات في البداية موجهة نحو المبادئ الأساسية للإنترانت، وكيفية الاستفادة منها، ولكن لوحظ فيما بعد أن الطلبات تميل شيئاً فشيئاً إلى التخصص وطلب معلومات من مستوى أعلى.

6-1-2 إدارة وصيانة الشبكة

إن اختيار مديري الإنترانت، وطريقة عملهم، هي أمور تُحدَّد على مستوى عالٍ نظراً لكونها تتعلق بسياسة الشركة، وطريقة توزيع الحسابات بين المستخدمين، وسماحيات الوصول، وطريقة استخدام الإنترانت. فقد تقرر الشركة استخدام أكثر من مدير واحد (بغية توزيع السلطة على الإنترانت)، أو تكتفي بمدير واحد يشرف على كل شيء. إن مهمة مديري الإنترانت متعددة الوجوه، فعليهم إدارة المعلومات على الموقع، وحل المشاكل والتضاربات، وتقديم الدعم التقني، والتحكم بطريقة تدفق المعلومات والاتصالات عبر الإنترانت و... وهذا ما يفرض شروطاً ومهارات خاصة يجب أن تتوفر في كل مدير، وتدريباً من طبيعة مختلفة عن التدريب الذي تحدثنا عنه آنفاً.

في هذا القسم، سنقوم بالتعريف بعمل المديرين من أجل إدارة وصيانة الإنترانت، وبماهية الشروط الواجب توفرها في كل مدير. كما سنشير باقتضاب إلى الدورات التدريبية الخاصة التي يجب أن يخضعوا لها.

آ- وظائف مديري الإنترانت (Administrators)

يوجد الكثير من الأعمال المطلوبة من مدير الإنترانت على أي موقع كان، وسنتطرق فيما يلي لبعض هذه المهام:

1- توزيع الحسابات والصلاحيات

يجب على مديري الإنترانت أن يعطوا لكل مستخدم حساباً وكلمة سر. يكون اسم الحساب عمومياً، أما كلمة السر فيُفترض أن تكون خاصة بصاحب الحساب فقط.

تلعب سياسة الإنترانت الأمنية دوراً هاماً في تحديد كلمات السر، ففي الإنترانت التي تكون درجة الأمن فيها منخفضة، يمكن أن تُستخدم أي كلمة سر يُحددها المستخدم، أما في الإنترانت ذات درجة الأمن العالية، فيمكن أن يفرض المديرون شروطاً على كلمة السر، مثل الطول وضرورة استخدام أرقام وأحرف خاصة مثل (_)، وذلك بهدف تعقيد كلمة السر، ويمكن أن تُغيّر هذه الكلمة كل فترة زمنية يمكن أن تقصر أو تطول حسب الحاجة الأمنية للشركة. في الإنترانت التي تعمل وفق قواعد وحدود صارمة، يمكن للمديرين أن يحددوا كلمات السر للمستخدمين، ولا يسمحوا لهم بتغييرها.

إن توزيع المستخدمين على مجموعات، وإعطاء درجات سماحية مختلفة للوصول إلى المعلومات على الإنترانت، هو العمل المكمل لإعطاء الحسابات. فيجب التنبه دوماً إلى أن هنالك هدفاً محدداً لدخول المستخدمين إلى الإنترانت، ولا يُفترض أن يعرف المستخدمين جميع الأمور على الإنترانت. كل مستخدم له عمل يقوم به، ويحتاج إلى مجموعة من المعلومات لأداء عمله. يجب على مديري الإنترانت أن يُجمّعوا المستخدمين ضمن مجموعات، ويتيحوا لكل مجموعة صلاحيات خاصة مناسبة لأداء عملهم. لنفترض مثلاً حالة شركة فيها قسم للذاتية يرعى شؤون العاملين، يجب على موظفي الذاتية أن يتمكنوا من الوصول إلى البيانات التي تحوي أضابير الموظفين، إذن يجب أن يُجمّع هؤلاء الموظفون ضمن مجموعة خاصة، ويُعطوا صلاحية الدخول إلى تلك البيانات. من ناحية أخرى، قد لا يكون لهذه المجموعة أي علاقة بأمور الرواتب والتعويضات، لذا يجب حجبها عنهم.

توجد درجات للسماحية أيضاً، فمثلاً يمكن للعاملين في مجموعة ما أن يصلوا إلى المعلومات، لكن للقراءة فقط، ودون إمكانية للتغيير فيها. فمثلاً، القرارات التي يُصدرها المدير العام، لا يجب لأحد غيره أن يتمكن من التعديل فيها، إلاّ أنه يمكن لأي شخص ضمن الشركة الاطلاع عليها متى شاء.

بإمكان مديري الإنترانت الوصول إلى أي معلومة في الإنترانت، لكن يجب عليهم أن يراعوا الوضع الذي هم فيه، ففي إمكانهم الوصول إلى أي معلومة عن أي مستخدم، واستخدام هذه المعلومات لأغراض لا تبررها ضرورات العمل أمر مرفوض تماماً. إن الثقة بين المستخدمين ومديري الإنترانت أمر هام جداً لنجاح الإنترانت، فبوجود هذه الثقة، سيشترك المستخدمون في الإنترانت، وبزوالها سيعزف المستخدمون عن استخدامها.

تشكل سلطة مديري الإنترانت، وقدرتهم على الوصول إلى أي معلومة من معلومات الشركة، مصدر قلق للكثير من الشركات. فهي تخشى دائماً من سوء الاستخدام، أو الاختراقات التي يمكن أن تحدث عبر هؤلاء المدراء. وتعمد بعض الشركات إلى توزيع المهام بين مديرين؛ فتسمح لأحدهم بالتحكم بالأمور التقنية مثل الدعم التقني وكلمات السر مثلاً، وتعطي الآخر إمكانية التحكم وإدارة ما يتعلق بعمليات الاتصال والتخاطب والمؤتمرات عن بعد.

2- *دراسة وتحليل العمل على الإنترانت*

توجد لدى مديري الإنترانت قاعدة بيانات عن جميع الأعمال التي يقوم بها مستخدمو الإنترانت تُسمى سجل العمل (Log File)، وعلى مديري الإنترانت الرجوع إلى هذه البيانات دورياً من أجل تحليلها واستخلاص نتائج تفيدهم في عملهم.

تسمح عمليات التحليل التي تجري على سجل العمل بمعرفة ما يجري على الإنترانت من وجهة نظر المستخدمين. فمن خلال سجل العمل، تمكن معرفة أكثر الأمور أهمية للمستخدمين، وهي المعلومات التي يزورونها باستمرار، كما تمكن معرفة الأمور التي لا يهتمون بها، وبالتالي يجب تحسينها. لنفترض أن شركة ما تضع معلومات عن موضوع معين على الإنترانت، وترغب بأن يطلع عليها جميع المستخدمين. لكن وبنتيجة تحليل سجل العمل، وجدت الشركة أن عدداً قليلاً من المستخدمين فقط يطلعون على هذه المعلومات. يمكن تحسين الوضع بأن يقوم الفريق المسؤول عن إعداد المعلومات بتغيير طريقة العرض لجعلها أكثر متعةً وجمالاً، وقد يحتاج إلى تعديل طريقة صياغة المعلومات، التي قد تكون مشكلتها في كونها على درجة عالية من التعقيد، فيجعلها مبسطة وسهلة.

يمكن لمديري الإنترانت أيضاً القيام بتجارب خاصة على الإنترانت من أجل الحصول على معلومات عن أداء الشبكة ومدى اهتمام الناس بها. مثلاً يمكن فحص مدى اهتمام الناس بأن يرسل مدير الإنترانت رسائل E-mail إلى الأشخاص الراغبين بالاشتراك يعلمهم فيها عن خدمات إنترانت الشركة، ثم يراقب الفترة التي سيرد فيها هؤلاء الناس. طبعاً الفترة القصيرة تعني أن الناس متلهفون للاشتراك، وأن سمعة إنترانت الشركة جيدة. يمكن استخدام نفس الاستراتيجية لقياس اهتمام الناس

بمواضيع أخرى. كما يستطيع مديرو الإنترانت أن يُجروا استفتاءات على مواضيع مختلفة وخدمات موجودة على الإنترانت، من أجل معرفة مدى تقبل الناس لهذه الخدمات.

يمكن من خلال سجل العمل معرفة نقاط الخلل في الشركة، ومعرفة نقاط الضعف والثغرات. فمن مراقبة عمل المستخدمين، تمكن معرفة الصفحات التي تحوي ارتباطات تشعبية غير صحيحة، أو المواقع التي لا يمكن الوصول إليها. كما يمكن مراقبة عمليات التسلل والدخول غير الشرعي إلى الإنترانت، وكشف طرقها، وإغلاق الثغرات الموافقة.

3- *الدعم التقني*

يحتاج الكثير من المستخدمين، حتى بعد انتهاء الدورة التدريبية، إلى الحصول على بعض المعلومات عن طريقة استخدام بعض الأدوات. إنّ مديري الإنترانت هم الأشخاص المسؤولون عن الإجابة على تساؤلاتهم، وتقديم الدعم التقني لهم.

يجب أن تتوافر على الإنترانت نسخة إلكترونية حول طريقة استخدام مجموعة الأدوات الموجودة، وأن يكون بإمكان المستخدمين الوصول إلى هذه المعلومات بسهولة. كما أن وجود ملفات أسئلة وأجوبة FAQ أمر ضروري، سواء لفائدة المستخدمين أو لراحة مديري الإنترانت.

إن هذه التخاطبية بين المستخدمين ومديري الإنترانت أمر مهم في عمل الإنترانت وكفاءتها. وتحقيق هذا الأمر يستلزم أن يتمكن المستخدمون من الوصول إلى مديري الإنترانت دوماً. كما تسمح هذه التخاطبية لمديري الإنترانت بالاطلاع على مشاكل المستخدمين، ومعرفة الخلل في الإنترانت، على نحوٍ دائم ومستمر.

4- *صيانة وأرشفة معلومات الإنترانت*

الهدف من عملية صيانة وأرشفة المعلومات هو تسهيل العمل على المستخدمين. تتضمن هذه العملية مسح الموقع مسحاً دائماً، وإضافة المعلومات الجديدة على نحوٍ متناسق مع بناء الموقع، وبما لا يؤثر

على معلومات الموقع الأخرى، كما تتضمن تحديث المعلومات القديمة، وإضافة معلومات حديثة مكانها، أمّا النسخ القديمة فيجب أرشفتها أو التخلص منها.

تتصف عملية الأرشفة بأنها عملية تفاعلية مع المستخدمين، فهي تجري وفقاً لسلوك المستخدمين تجاه المعلومات المتوفرة. فالمعلومات التي لا يزورها أحد، التي جرى تحديدها من تحليل المعلومات في سجل العمل، يمكن أرشفتها وإزالتها من الموقع، وفي بعض الأحيان يمكن حذفها.

نجد التفاعل مع المستخدمين أكبر فيما يتعلق بصيانة الموقع، فالمستخدمون يكونون على اتصال أكبر بالمعلومات التي يبحثون عنها، بالتالي يتعرضون للمشاكل التي يمكن أن توجد ضمن بعض الصفحات (ارتباط تشعبي فيه خلل، معلومات ناقصة، مشاكل في استعراض الصفحة،...). إن الرسائل التي ترد من المستخدمين عن هذه الأخطاء لها دور كبير في صيانة الموقع. من ناحية أخرى، ولأن الوقائع تقول أن المواقع يزداد حجمها مع مرور الوقت، فستصبح عملية الصيانة عملية صعبة، وهذا ما يستلزم في بعض الأحيان استخدام برمجيات خاصة من أجل المساعدة في عمليات الصيانة. وفي كثير من الأحيان يجد مديرو الإنترانت أن من الواجب إضافة مجلدات فرعية ضمن مجلد قديم، لأن المعلومات أصبحت كثيرة وقد تؤدي إلى ضياع المستخدم ضمنها، مما يستلزم إعادة تنظيمها من جديد.

ب- المهارات المطلوبة من المديرين

يجب أن تحرص الشركة عند اختيار مديري الإنترانت أن تتوافر فيهم مجموعة من الشروط التي تؤهلهم للقيام بعملهم بكفاءة، فالمعلومات التقنية الجيدة أمر أساسي، لكن يجب الأخذ بعين الاعتبار قدرة مدير الإنترانت على التعامل مع الناس وإدارتهم إدارةً جيدةً. ومن الخطأ تغليب الجانب التقني على الجانب الاجتماعي، ففي كثير من الأحيان، يكون مدير الإنترانت على تماس مع الناس ويجب أن يتصرف تصرفاً مناسباً. في الأحوال المثالية، يجب على مدير الإنترانت أن يتحلى بالصفات والمهارات التالية:

▪ *المهارة التقنية*

كما هو الحال مع الأمور التقنية الحديثة، لا بد من وجود شخص يفهم ما يجري، ويستطيع تفسيره وتطويعه. فالإنترانت لا تزال حديثة، ولا تزال الخلفية التقنية عند الناس ضعيفة، لذا لا بد من أن تكون لدى مدير الإنترانت خلفية تقنية متينة عن الإنترانت: ما هي، كيف تعمل، ماذا يوجد في الداخل، وحتى ماذا يوجد خارج الإنترانت... فمدير الإنترانت هو الشخص المنوطة به الإجابة على أي تساؤلات، ومتابعة التطورات الحديثة في شتى المجالات المتعلقة بالإنترانت.

يجب على مدير الإنترانت أن يُلمّ بالتغيرات التقنية على المواقع الأخرى في العالم، وهو ما يتطلب منه متابعة دائمة لما يجري فيها. كما يجب عليه أن يضع الخطط والمشاريع لتطوير العمل على الإنترانت وتحسينه وأتمتته، فمثلاً يمكن أن ينشئ برنامجاً صغيراً من أجل الإعداد لمؤتمر فيديوي بدلاً من القيام بالعمل يدوياً كل مرة.

ينبغي على مدير الإنترانت أن يكون واسع الاطلاع على أمور البرمجيات التي يمكن استخدامها على الإنترانت، مثل المستعرضات. فيجب عليه أن يعرف الفروق بين مختلف أنواع المستعرضات، وأن يحدّد حاجة الشركة، ويقرر على هذا الأساس ماذا ينبغي أن تشتري الشركة.

من الضروري أيضاً لمدير الإنترانت أن يكون على معرفة عميقة بالإنترنت، فالإنترانت شديدة الشبه بالإنترنت، وأن يعرف طرق الاتصال المختلفة وعبر جميع الأنظمة حتى يساعد المستخدمين على استخدام الإنترانت من أي مكان.

▪ *دقة الملاحظة*

من بين الأعمال المنوطة بمدير الإنترانت، توجد أعمال تتطلب دقة وانتباهاً، مثل الارتباطات التشعبية. فمسؤولية صيانة الارتباطات التشعبية والتحقق من صحتها تقع على عاتق مدير الإنترانت، وأي خطأ في كتابة العنوان لن يوصل المستخدم إلى هدفه. تصبح الأمور صعبة أكثر عندما يكون مدير الإنترانت مسؤولاً عن إنترانت سريعة التغير (ديناميكية)، فالمطلوب منه هو الحفاظ دوماً على تناسق

المعلومات ضمن موقعه. في هذه الحالات يجب عليه أن يظل منتبهاً ومتوقد الذهن، لأن أي شاردة ستخل ببناء الموقع.

- *الذكاء الاجتماعي*

قلنا أن مدير الإنترانت هو الشخص الأكثر خبرة في الشركة بأمور الإنترانت، وهو من لديه إجابة على كل سؤال. لكن هذه المعلومات لن تكون مفيدة إذا لم تجد طريقها إلى عقول الناس. يوجد الكثير من الأشخاص من أصحاب الخبرات التقنية العالية جداً، لكنهم لا يستطيعون أن يشرحوا ماذا يفعلون لغيرهم، هذا النوع من الناس لا يصلح أبداً أن يكون في منصب مدير إنترانت.

يجب على مدير الإنترانت أن يكون شخصاً لبقاً هادئاً قادراً على شرح أصعب الأمور التقنية بأسلوب بسيط وواضح، ويستطيع تغيير أسلوب حديثه حسب سوية الأشخاص الذين يسألونه. يجب أن يتحلى بالصبر، فقد يتعرض لنفس السؤال من الشخص نفسه عدة مرات، وقد يصادف نوعيات مزعجة من الناس، لكن الصبر وهدوء الأعصاب هما رد الفعل الوحيد الصحيح.

إن عدم إجابة المستخدمين على أسئلتهم، أو الحديث معهم بطريقة غير مناسبة، أو الإكثار من التفاصيل التقنية أو غيرها من التصرفات التي قد تُشعر المستخدم الذي يسأل بعدم الراحة، هي أمور مرفوضة، ويجب أن يتجاوزها مدير الإنترانت، كما يجب أن يُشجع المستخدمين على زيارته، أو الاتصال به كلما دعت الحاجة، فهو الشخص الذي يلجؤون إليه في كل طارئ.

ج- دورات المديرين التدريبية

بعد أن تحدد الشركة استراتيجية الإنترانت، والأهداف التي تريد تحقيقها، يجب أن تختار مجموعة مديري الإنترانت، ثم تقيم لهم دورة تدريبية لتعريفهم بحاجات الشركة، واستراتيجيتها، وكيفية إدارة المواقع. كما يجب أن تتضمن الدورة معلومات تقنية عالية المستوى، وفي المجالات المطلوبة.

إن الإعداد لمنهاج الدورة أمر ينبغي التخطيط له مسبقاً أثناء إعداد مشروع الإنترانت. ويمكن أن يُبنى المنهاج من مجموعة من المواضيع في التكنولوجيا المتقدمة، وHTML وطرق الاتصال، ومجموعة من المواضيع الأخرى الأساسية في عمل الشركة. كما أن استراتيجية عمل الموقع ونوعه أمور أساسية في اختيار المنهاج وتحديد مدة الدورة، فمثلاً إذا أرادت الشركة للموقع أن يعمل كموقع HTML على الوب، فيكفي تعليم مديري الإنترانت في ذلك الموقع طريقة إدارة الموقع وصيانته، وهو أمر قد لا يستغرق سوى بضعة أيام، أما تعلم لغات برمجة وطرق إدارة قواعد البيانات (في حال احتواء الموقع على قاعدة بيانات ضخمة)، فهي أمور قد تتطلب زمناً طويلاً.

يجب أن يتعلم مديرو الإنترانت في الدورة أيضاً كيفية إظهار الإنترانت كأداة فعالة، وليس فقط كيف يبنون المواقع ويديرونها. كما يجب أن يُشاركوا في إعداد منهاج دورات العاملين فيما بعد، وحتى أن يُسهموا في التدريس إن أمكن. فبهذا العمل، يتدربون هم أنفسهم ويتعلمون من الاحتكاك المباشر بالمستخدمين، فيعرفون حاجاتهم، وتساؤلاتهم، ويمكنهم إدارة المواقع التي تحت سلطتهم بصورة أكثر كفاءة.

كما يجب الاعتماد على حب مديري الإنترانت للتعلم الذاتي، لذا يجب أن تسمح الشركة لهم باستخدام جزء من المخدّم على الإنترانت لأغراض تدريب أنفسهم. في هذا المكان، يمكن لمديري الإنترانت أن يختبروا التقنيات الجديدة ويتقنوها. لقد أثبتت هذه الطريقة أهميتها في عمل مديري الإنترانت، فالكثير منهم تعلم من تلقاء نفسه الكثير من المعلومات التقنية المتقدمة.

د- طريقة انتقاء مديري الإنترانت

بعد أن تحدثنا عن مديري الإنترانت، وأعمالهم، وواجباتهم، وما هي الصفات الواجب التحلي بها، نجد أنه من المفيد أن نتحدث عن طريقة انتقاء الشركة لمديري الإنترانت التي تملكها. يجب أن تكون عملية الانتقاء مدروسة بعناية، ويجب الانتباه إلى أن الشخص الأكثر خبرة ليس دوماً هو الشخص المناسب. كما تلعب استراتيجية الشركة، ونوع الموقع دوراً أساسياً في اختيار مديره. سنحاول شرح ذلك من خلال المثالين التاليين:

مثال 1

شركة تريد عرض منتجاتها على أحد مخدّمات الإنترانت الخاصة بها. كما تريد أن تنشر المقالات والمواضيع التي تتعلق بالمواد التي تنتجها، إضافة إلى معلومات عن نشاطها التجاري، والأخبار الجديدة عنها.

مثال 2

تريد الشركة السابقة أن تدير قواعد البيانات في الشركة عن طريق الإنترانت، كما تريد أن تنشئ وسط عمل تشاركي من أجل إنجاز المشاريع الكبيرة التي يتطلب تحقيقها عدة فروع. ستضع هذه الخدمات على مخدّم آخر من مخدّماتها على الإنترانت.

يختلف المخدّمان السابقان عن بعضهما في أن لكل منهما وظيفة ومهمة مختلفة. فالمخدّم الأول يعمل كمخدّم وب، وعملية إدارته لن تحتاج إلى مدير على مستوى من التأهيل والمعرفة التقنية مثل مدير المخدّم الثاني، الذي يحتاج إلى مستوى تأهيل عالٍ من حيث المعرفة التقنية والخبرة العملية حتى يتمكن من تنظيم مهمات العاملين، وتوزيع الصلاحيات، و.... بسبب هذا الاختلاف في الوظائف بينهما، يجب انتقاء مديرَين مختلفين، كما يجب الانتباه إلى أن وضع مدير الموقع الثاني مكان مدير الموقع الأول يُعتبر قراراً خاطئاً، فهو سيكون على مستوى تقني أعلى من الموقع الذي سيعمل فيه.

حتى تتمكن الشركة من تحديد عمل مدير الإنترانت، يجب أن تجيب على الأسئلة التالية:

- ما هو الهدف العام للإنترانت ؟، هل هو عرض معلومات ؟، أو هل هو إتاحة وسيلة تخاطبية متطورة بين المستخدمين ؟

- ما هي المعلومات التي ستُعرَض على الإنترانت ؟. تسمح بعض الشركات بعرض أي نوع من المعلومات، وتشجعها، في حين يحدّد البعض الآخر أنواعاً معينة فقط. يمكن للمعلومات أن تكون أخباراً أو مقالات عن المواضيع التي تدعمها الشركة، كما يمكن أن تكون محادثات صوتية، أو فيديوية، أو دراسات أو مواعيد لاجتماعات.

- من هم المستخدمون الذين سيعملون على الإنترانت ؟. تجب معرفة نوعية المستخدمين، ومستوى معارفهم. طبعاً سيُوزَّع هؤلاء المستخدمون ضمن مجموعات، لكل منها صلاحيات مختلفة بما يكفل سير العمل سيراً جيداً. هذه الصلاحيات تكون من نمط قراءة بيانات فقط، تعديل البيانات، إمكانية المشاركة في المؤتمرات، إمكانية استخدام خدمات معينة (الوصول إلى الإنترنت مثلاً).
- كيف يُتوقّع لكل مجموعة من المستخدمين أن تستخدم الإنترانت ؟. يجب تحديد عمل كل مجموعة من المستخدمين، وما هو المطلوب حتى تنفذ عملها، هل تحتاج المجموعة إلى الوصول إلى موارد مشتركة مع مجموعات أخرى، هل تحتاج إلى استخدام الخدمة الفلانية ؟
- من سيزود الموقع بالمعلومات ؟. هل قسم المبيعات هو من سينشر تقاريره على الإنترانت فقط ؟، أم هو قسم التصميم ؟، أم الاثنان معاً، وما طبيعة المشاركة بينهما ؟ ...

عندما تتمكن الشركة من الإجابة على الأسئلة السابقة، فبإمكانها الانتقال إلى مرحلة انتقاء مديري الإنترانت حسب العمل المطلوب. ومن بين المرشحين، تختار المرشح ذا الذكاء الاجتماعي المتميز والمعرفة التقنية العالية، وتراعي الصفات والمهارات الواجب تحليه بها والتي تحدثنا عنا سابقاً. بعد اختيار المدراء، تدربهم على الأعمال التي حددتها من خلال الأجوبة على الأسئلة السابقة، وتوكل إليهم مهامهم الجديدة.

هـ- تجارب الشركات في تأهيل مديري الإنترانت

شركة *The Sporting Goods and Apparel Association (SGAA)*

أشرنا في السابق إلى عمل هذه الشركة في ميدان تأهيل العاملين، ونكمل الحديث هنا عن الأعباء الأُخرى التي تحملتها الشركة نتيجة استخدامها للإنترانت.

استقدمت الشركة في البداية ثلاثة خبراء لإدارة إنترانت الشركة، وأوكلت إلى كلٍ منهم جزءاً من المسؤوليات والسلطات. كان دور الخبير الأول (مدير الإنترانت) الاهتمام بالمستخدمين، من تقديم الدعم التقني والإجابة على أسئلتهم، إلى العمل مع المستخدمين لتحديث واجهات الاستخدام في الموقع. كما كان من مسؤولياته وضع نسخة إلكترونية عن دليل استخدام الأدوات على الإنترانت، وملفات المساعدة (Help Files)، إضافة إلى مراقبة اهتمامات المستخدمين من خلال سجل العمل.

أمّا الخبير الثاني، فكان واجبه أن يهتم بمحتوى الموقع، من جمع المعلومات وإنشائها، والاهتمام بنوعيتها، ونشرها على الإنترانت. كان عمله مشابهاً لعمل أمين المكتبة، فعليه معرفة أين توجد كل معلومة، وكيفية الوصول إليها، والاهتمام بصلاحية المعلومات، وتناسق الموقع، والتأكد من عدم وجود ارتباطات تشعبية خاطئة.

كانت مهمة الخبير الثالث الاهتمام بالبرمجيات. وكان عمله يقتضي تطوير برمجيات خاصة بالإنترانت، إضافةً إلى التأكد من جاهزية البرمجيات الموجودة، ومتابعة التطورات التقنية في العالم، والجديد في عالم البرمجيات ممّا يمكن أن يفيد في تحسين عمل الإنترانت.

كان عمل الخبراء الثلاثة ناجحاً من وجهة نظر الشركة، وقد لاحظت وجود إقبال على الإنترانت، ورضى من العاملين لديها، مما يعني أن الإنترانت التي كانوا يديرونها كانت ناجحة، وحققت الهدف المطلوب من وجودها. طبعاً هذا لا يعني أن كل شيء قد انتهى، فالإنترانت تحتاج إلى عمل مستمر، وجهد يومي من أجل الحفاظ على نجاحها.

6-2 انعكاسات الإنترانت على أداء وإنتاج الشركة

تُوظّف الشركات الكثير من الأموال على إنشاء الإنترانت وتشغيلها، وذلك بهدف تحسين أدائها وإنتاجيتها، وتسهيل طرق العمل وتطويرها. ونذكّر بأن الفوائد التي تُقدمها الإنترانت تندرج ضمن مجموعتين كبيرتين هما:

- **الفعاليـة:** وتعـني تحسـين تقنيـات تبـادل المعلومـات مـن حيـث التغلـب علـى صعوبـات الاتصالات من جمع ونشر ونقـل المعلومـات الضروريـة بسـرعة. وتتجلـى بالتأثـير علـى أداء وإنتاج الشركة.
- **الفاعلية:** وتعني التطور الإداري الحاصل نتيجة الاستفادة من الاتصالات المتطورة في إقحـام أكبر عدد ممكن من العاملين في عملية اتخـاذ القـرار. وتتجلـى بالتأثـير علـى منهجيـة عمـل الشركة وإدارتها.

سنحاول في هذا القسم أن نلقي بعض الضوء على الفوائد التي تجنيها الشركات من وجـود الإنـترانت فيها، ونبين الطرق الجديدة في العمل التي حلت مكان الطرق القديمة. أي أننا سنتحدث عن الفوائـد التي تندرج ضمن فئة الفعالية فقط. بينما سنتحدث عن الفاعلية في القسم التالي.

تُصمم الشركة الإنترنت حسب حاجتها الحالية والمستقبلية، وتُشغِّل الشبكة بما يلبي هذه الحاجات. وبحسب طرق التشغيل، يمكـن تصنيـف شـبكات الإنـترانت إلى ثلاثـة مسـتويات، نرتبـها تصاعديـاً حسب درجة التعقيد:

6-2-1 عرض المعلومات العامة

لا توجد شركة في العالم مهما صغرت أو كبرت، وإلا ولديها معلومات ترغب بعرضـها علـى العمـوم، سواء من موظفيها أو شركائها أو زبائنها. فبعض الشركات تعرض إحصائيات عن عملها خلال العام، وما هي التطورات التي حققتها، وأخـرى تعـرض معلومـات عـن المنتجـات الجديـدة الـتي تنتجـها، وغيرها تهتم بنشر معلومات عن القوانين الناظمة في الشركة، و...

إن الفوائد التي تُقدمها الإنترانت ضمن هذا المستوى كثيرة، سنقسمها إلى فئتين حسـب الجهـة الـتي تستفيد من الإنترانت، وهما: الزبائن والعاملين. توجد أقسام في الشركة شديدة الصلـة بالزبـائن، لـذا سنستثني هذه الأقسام من فئة العاملين، وسنتحدث عنها في فئة الزبائن، فكـل تعديـل في عمـل هـذه الأقسام له انعكاس مباشر على الزبائن.

آ- الانعكاسات على الزبائن

تتجلى العلاقة بين الزبائن والشركة من خلال قسم التسويق. وفي الشركات التي لا تملك إنترانت، تقع على عاتق هذا القسم مجموعة كبيرة من الأعمال الواجب إنجازها مثل قيادة الحملات الإعلانية لمنتجات الشركة، وعرض المنتجات، والاتصال بالوكلاء. كما تجب عليه معرفة أراء الزبائن، وإجراء دراساته عن المواد المعروضة و متطلبات السوق، والتعامل مع الوكلاء والموزعين المعتمدين.

يُضيف استخدام الإنترانت في التسويق فائدة كبيرة إلى هذا القسم، فعن طريق الإنترانت تُصبح الاتصالات أسهل، بفضل أدوات الاتصال المتطورة، كما أن عرض البضائع يُصبح أسهل من ذي قبل، وكذلك الإعلانات. يمكن لهذا القسم الاتصال مع مواقع على الوب أو إنترانت أُخرى من أجل وضع إعلانات على موقعهم، إضافة إلى الإعلانات على مواقع الإنترانت الخاصة بالشركة. كما أن عملية عرض البضائع تصبح أسهل من قبل، فموقع قسم التسويق يحتوي عن عرض كامل لجميع منتجات الشركة، ويستفيد من إمكانات العرض المتميزة التي تُقدمها صفحات HTML، ومن طريقة العرض المعتمدة على إمكانية تجول الزبون حسب حاجته، وليس حسب بنية يفرضها فريق التسويق. يمكن الحصول على أراء الزبائن بسهولة وراحة عند استخدام الإنترانت، فكل ما هو مطلوب من الزائر هو أن ينقر على ارتباط تشعبي ضمن إحدى الصفحات من أجل كتابة رسالة إلى فريق التسويق يعبر فيها عن رأيه وملاحظاته، ويرسلها باستخدام E-mail. إن استخدام الإنترانت لا يعني إلغاء الوسائط الأُخرى مثل التلفاز أو الجرائد، بل مع الازدياد المستمر في عدد مستخدمي وزوار الإنترانت، تظهر نتائج التسويق بوضوح مما ينعكس إيجاباً في عمليات البيع.

بإمكان الزبائن (أو الموزعين) أن يطلعوا على المعلومات التي تهمهم بسهولة أيضاً، فسابقاً كان عليهم إمّا التوجه إلى أحد مكاتب الشركة المختصة، أو الاتصال بالهاتف، وتوجيه أسئلة لفترة قد تطول، أو أحياناً السعي إلى الحصول على كراس عن الشركة. بوجود الإنترانت، يستطيع الزبون زيارة الموقع الخاص بالتسويق، وفيه يجد كماً كبيراً من المعلومات عن كل ما يريد أن يعرف عنه (إذا كان الموقع مبنياً جيداً). يمكنه الاطلاع على منتجات الشركة وخواصها، ومواصفاتها، والاطلاع على المقالات

المنشورة في وسائل الإعلام عن هذه المنتجات. كما يستطيع الاطلاع على المنتجات الجديدة التي ستصدر قريباً وموعد وجودها في الأسواق. كما يمكنه الحصول على عناوين الموزعين وأرقام هواتفهم.

في الشركات التي لا تملك إنترانت، يجمع فريق التسويق آراء الزبائن من خلال استطلاعات للرأي يقوم بها بين فترة وأخرى، كما يساهم موزعو الشركة في تزويده بمتطلبات الزبائن وحاجات السوق. مع وجود الإنترانت، يستطيع الزبون أيضاً، باستخدام الإنترانت، التأثير على قرارات الشركة وخططها القادمة، من خلال إبداء رأيه في المنتجات المعروضة، واقتراح تعديلات مناسبة. فالنقطة الأساسية بوجود الإنترانت هي إلغاء هذا التسلسل الهرمي لنقل المعلومات من الزبائن إلى مناطق اتخاذ القرار. باتباع هذا الأسلوب الجديد، يمكن لمجموعة الدراسات في قسم التسويق أن تُعطي تقييماً يومياً عن حالة السوق ومتطلبات الزبائن، كما يمكنها طرح استطلاعات للرأي على الإنترانت حول أمور محددة.

لنأخذ حالة شركة برمجيات تطرح تطبيقاً برمجياً جديداً، كما هو الأسلوب المتبع، بعد إجراء مجموعة من الاختبارات. لكن هذه الاختبارات غير كافية لكشف جميع المشاكل في هذا التطبيق البرمجي. تعتمد الشركة اعتماداً أساسياً على الزبائن في عملها، فهي تحتاج إلى آراء الزبائن وتعليقاتهم عن التطبيق الجديد، كما تحتاج معلومات من الزبائن عن الأخطاء الموجودة من أجل تصحيحها في النسخ اللاحقة. إن استخدام الإنترانت في عمل هذه الشركة، يحقق لها فائدة كبيرة من حيث قدرتها على تلقي رغبات الزبائن وكشف الأخطاء الموجودة في تطبيقاتها، وبالتالي الاستمرار في عملها بنجاح.

للإنترانت تأثير أيضاً على الموزعين المعتمدين. إذ يوجد هؤلاء الأشخاص عادةً في أدنى السلم الهرمي للشركة، والاهتمام بهم يكون قليلاً، وعلاقتهم محصورة بمجموعة من الأشخاص (ليسوا على درجة رفيعة في الشركة)، مما يُشعرهم بعدم الانتماء للشركة. مع الإنترانت، يمكنهم الاطلاع أكثر على ما تقوم به الشركة، وعلى نشاطاتها الجديدة ومشاريعها المستقبلية، كما يمكنهم أن يوصلوا آراءهم إلى جهات أعلى في الشركة. تُكسب هذه الأمور مجتمعة هؤلاء الموزعين شعوراً بالانتماء للشركة، مما يساهم في تحسين أدائهم وعملهم.

توفر الشركة باستخدام الإنترانت مجموعة من النفقات التي كانت ضرورية سابقاً، مثل تكاليف طباعة كتيبات تعريف بالمنتجات الجديدة، كما توفر الكثير من المكالمات الهاتفية والفاكسات ذات السعر المرتفع (مع الموزعين مثلاً)، وتستبدل بها بالاتصالات الأرخص ثمناً، والأكثر جودة، باستخدام الإنترانت. ولا ننسَ طبعاً أن الشركة قد دفعت ثمناً لإنشاء الإنترانت، ويجب أن تعوضه من خلال الاستثمار الجيد لها.

ب- الانعكاسات على العاملين في الشركة

تُفيد الإنترانت كثيراً في أمور الاتصالات، وهو ما يحتاجه العاملون بكثرة أثناء العمل. ففي كثير من الأحيان يجب على العاملين في السكرتارية الاتصال بمدراء الأقسام لتحديد مواعيد اجتماعات أو لتعديل مواعيد سابقة، كما يُضطر العامل أحياناً إلى معرفة بعض المعلومات عن وضعه في الشركة. إن استخدام الإنترانت في الشركة، يسمح بالقيام بعمليات اتصال سهلة ومريحة، وسريعة أيضاً، وهو ما يحل مشكلة ازدحام خطوط الشركة الدائم.

فيما عدا الاتصالات، يحتاج العاملون إلى مجموعة كبيرة من الوثائق، فهم بحاجة إلى كتيبات تشرح طريقة عمل البرمجيات التي يستخدمونها (دليل الاستخدام)، وإلى وثائق تشرح قانون الشركة وأهدافها، وإلى دليل هواتف ضمن الشركة وهواتف العملاء. إن طباعة هذه المعلومات تُكلف الشركة مبلغاً كبيراً كل عام، وتجب إعادة طباعتها كلما طرأ عليها جديد. تُقدّم الإنترانت الحل الأفضل لشكلة الوثائق اللازمة، فيمكن وضع نسخة إلكترونية وحيدة على الإنترانت، والسماح لجميع العاملين بالوصول إليها.

من ناحية أخرى، يمكن وضع معلومات كثيرة عن الشركة على الإنترانت، وإتاحتها للجميع، مثل معلومات عن الضمان الاجتماعي للعاملين، وسياسة الشركة الحالية والمستقبلية، والنظام الداخلي، ومقالات ومواضيع متعلقة بالشركة. كما يمكنها العمل على تشكيل نوع من التفاهم المشترك مع العاملين من خلال نشر مواضيع معينة توضح أفكارها وتصرفاتها.

إن استخدام الإنترانت يوفر وقت العاملين في الشركة، ففي قسم الذاتية، ينفق العاملون قسماً لا بـأس به من وقتهم في الإجابة على أسئلة العاملين المتعلقة بوضعهم الوظيفي وإجازاتهم وغيرها مـن الأسئلة التي تتكرر من قبل معظم العمال. بوجـود الإنـترانت، يمكـن وضـع نسـخة إلكترونيـة عـن مجموعـة الأسئلة المكررة مع أجوبتها، مما يوفر وقت العاملين ويمكّنهم من الانصراف لأمور العمـل. كذلـك هـو الحال مع الأقسام التي تُقدم المعلومات للمستخدمين، مثل قسم التدريب والتأهيل، والذي يتصل معـه العاملون من أجل توجيه أسئلة تقنية لحل المشاكل التي تُصادفهم.

لا بد وأن التوفير في المصاريف قد بدا واضحاً للقارئ، فالشركة لن تحتاج إلى طباعة نسـخ كثـيرة عـن طرق استخدام البرامج، ولا طباعة تعليمات العمل. فكل ما هو مطلوب هو أن تُجهّز نسخة إلكترونيـة وتضعها على الإنترانت. كما أن الاتصالات أصبحت أكثر سهولة وأقل تكلفة، ولم تعد خطوط الشركة مشغولةً دوماً كما كانت في السابق.

6-2-2 المشاركة في بيانات العمل

بيانات العمل المشتركة هي البيانات التي تحتاجـها أكثر مـن جهـة في الشـركة، وتملـك سماحيـات مختلفة للتعديل عليها والقراءة منها. إذن عند استخدام بيانات عمل مشتركة، يجـب إيجـاد وسـائل لضمان عدم تعارض هذه الجهات بعضها مع بعض أثناء استخدام هذه المعلومات، مثل استخدام نظام قواعد بيانات لإدارة هذه البيانات. يضمن استخدام الإنترانت من أجل المشاركة في بيانات العمل أنها تُستخدم من أجل عرض المعلومات العامة، أما قرار تحديد مسـتوى اسـتخدام الإنـترانت والإمكانـات المتاحة فيجب أن يُتخذ على أساس حاجة الشركة في الوقت الراهن وفي المستقبل. تمكـن ملاحظـة أن المستوى الأول (في جزء منه) هو حالة خاصة من المستوى الثاني الذي يسـمح بدرجـة تشـارك أكـبر، فهو يمثّل الحالة التي تكون فيها كافة السماحيات معطـاة للشـركة، بينمـا لا يملـك الآخـرون سـوى سماحية القراءة.

آ- الانعكاسات على الزبائن

إن المعلومات التي أشرنا إليها في المستوى الأول هي معلومات إما دائمة، مثل النظام الداخلي للشركة، أو شبه دائمة أي تظل دون تغيير لفترة طويلة (نسبياً)، مثل استراتيجيات الشركة. لكن توجد في الشركة معلومات تتغير بسرعة، وتريد عرضها على المستخدمين. حتى تتمكن الشركة من عرض هذه المعلومات، فإنها تربطها بنظام قواعد بيانات مثل Oracle، وتعكس التغييرات التي تجري على قاعدة البيانات، على الصفحات المعروضة للمستخدمين (زوار الموقع). إن استخدام قاعدة البيانات المشتركة هذه، يسمح للشركة بأن تعرض معلوماتها على نحوٍ سريع وفوري، ودون الحاجة لأي اتصالات، أو انتظار لأي معلومة حتى تصل من أحد الأقسام التي تزود القاعدة بالمعلومات.

يستفيد الموزعون كثيراً من ميزة وجود بيانات مشتركة على الإنترانت، فبدون هذه الميزة، يجب عليهم إما تنظيم اجتماعات منفردة من أجل تبادل الآراء والخبرات، أو انتظار الاجتماع السنوي (إن وجد)، فالشركة لا تكون مهتمة كثيراً بعقد اجتماعات فيما بينهم لأنها تعتبرهم ملحقين بها، وليسوا جزءاً منها. في حال استخدام بيانات مشتركة، يمكن لكل موزع أن يضيف إلى قاعدة البيانات هذه مجموعة من المواضيع التي تهمه، وأن يضع التجارب الهامة التي حدثت معه خلال الفترة الماضية. كما يمكن ترتيب لقاءات واجتماعات وجداول العمل والخطط الزمنية بسهولة أكبر. لنفترض أن هؤلاء الموزعين استخدموا E-mail من أجل ترتيب جدول الأعمال، عندها يجب إرسال نسخة إلى جميع الموزعين، وفي حال إجراء أي تعديل عليه، يجب إرسال التعديل إلى الجميع. في حال استخدام قاعدة بيانات مشتركة، يصبح جدول الأعمال في مكان واحد فقط، وفي حال التعديل عليه فالأمر بسيط جداً ؛ فتعديل قاعدة البيانات يجري في مكان واحد فقط، أما باقي الموزعين، فسيجدون التغييرات حالما يتفحصون قاعدة البيانات. إذن الإنترانت تسمح للموزعين، وبأقل تكلفة للشركة، بأن يتبادلوا الخبرات والمعلومات عن السوق والمنتجات. إن في زيادة الخبرة لدى الموزعين فائدة للشركة والموزعين على حد سواء،و من شأنها أن تساهم في زيادة إنتاجية الشركة.

ب- الانعكاسات على العاملين في الشركة

لعل الانعكاسات على العاملين في الشركة أكثر أهمية منها على الزبائن، فباستخدام البيانات المشتركة بين العاملين، يمكن تجميع الخبرات في إدارة وتنفيذ المشاريع المتراكمة في قسم ما، وتوفير هذه الخبرات لجميع العاملين الذين يحتاجونها، مما يساهم في دفع عمل الشركة إلى الأمام.

تفيد قاعدة البيانات المشتركة في معرفة كل فرع من الشركة لحالة باقي الفروع، مما يسمح بتوزيع العمل عليهم، أو بطلب بعض المواد الموجودة في ذلك الفرع والتي يعاني فرع آخر من نقص فيها، أو بتخديم الزبائن. لنفترض حالة شركة لديها مجموعة من منافذ البيع في المدينة، وقد عملت الشركة على ربط هذه المنافذ بالإنترانت. إذا كان الضغط كبيراً على أحد المنافذ، وانتهى مخزون إحدى السلع عنده، فإن بإمكانه توجيه الزبائن الجدد الذين يطلبون هذه المادة إلى منفذ آخر، وبهذا تحتفظ الشركة بزبائنها. يستطيع أي منفذ بيع أن يعرف ما هي المواد الموجودة لدى منفذ البيع الآخر وكميتها، وذلك بفضل قاعدة البيانات المشتركة الموجودة على الإنترانت. ففي قاعدة البيانات هذه، يسجل كل منفذ بيع العمليات التي يقوم بها: ما هي المادة التي باعها، وما هي كميتها. إن هذه الخدمة مفيدة للشركة والزبائن، لكنها تُصبح أكثر فائدة للزبائن في حال تعلق الأمر بمواد هامة مثل الأدوية الطبية.

تُتيح قاعدة البيانات المشتركة على الإنترانت إمكانية تجاوز الإشكاليات الإدارية الناتجة عن تأخر وصول القرارات والأوامر الجديدة إلى جميع العاملين في الشركة. لنفترض أن شركة تبيع منتجاتها بسعر مخفض لمجموعة من الزبائن. وفي أحد الأيام قررت تغيير السعر، أو استثناء بعض الزبائن من التخفيضات، لكن هذا القرار لم يصل بعد إلى جميع المعنيين بذلك، مما جعلهم يستمرون بالبيع بنفس السعر القديم !. إن مشاكل من هذا النوع تُحل بسهولة باستخدام الإنترانت، فاستخدام قاعدة بيانات مشتركة لحفظ قرارات وأوامر الشركة، وربط البرمجيات التي يستخدمها العاملون من أجل إصدار فواتير البيع بها، كفيل بحل الموضوع. فعندما يُغير مدير الشركة بعض القرارات ضمن قاعدة البيانات المشتركة، فستنعكس هذه التغييرات مباشرة على فواتير البيع. لأن برنامج إصدار الفواتير يأخذ المعلومات من نفس قاعدة البيانات.

يمكن الحديث عن الكثير من الفوائد التي تجنيها الشركة من استخدام بيانات مشتركة ضمن الإنترانت الخاصة بها، مثل تنظيم جداول العمل، والخطط الزمنية للمشاريع، وذاتية الموظفين، وكثير غيرها ...

6-2-3 الاتصال التفاعلي

الاتصال التفاعلي هو الاتصال الذي يسمح لمستخدميه بالتخاطب فيما بينهم سواء بتوجيه الأسئلة أو بالرد عليها رداً حياً ومباشراً، والعمل معاً ضمن هذا الوسط. تسمح الإنترانت بمجموعة كبيرة من أدوات الاتصال التفاعلي، مثل المؤتمرات الفيديوية، والمؤتمرات الصوتية، وغيرها من الأدوات.

إن هذا المستوى هو المستوى الأعلى لاستخدام الإنترانت، والأكثر تطوراً، ويسمح بكثير من الأعمال والنشاطات ضمن الشركة، كما سنرى فيما يلي.

آ- الانعكاسات على الزبائن

تُقيم الشركات عدداً من المؤتمرات حول مواضيع تهم الشركة، مثل المنتجات الجديدة، أو شرح الاستراتيجية القادمة، أو حتى في بعض الأحيان مؤتمرات عن تقنيات حديثة تناقش وتشرح من خلالها التطورات الجديدة. يمكن للزبائن، في الحالات التي تسمح لهم الشركة بذلك، أن يُتابعوا هذه المؤتمرات التي تُقدم للمهتمين منهم معلومات جديدة ومفيدة.

يمكن للموزعين في الشركة أن يُقيموا بأنفسهم مؤتمرات على الإنترانت في حال سمحت لهم الشركة بذلك، ومن خلال هذه المؤتمرات يستطيعون تبادل الأفكار والمعلومات حول منتجات الشركة وتقبل الناس لها، وعن الطريقة الحديثة في العمل. كما يمكن أن يتبادلوا الخبرات ويناقشوا أهم المنجزات خلال الفترة المنصرمة، وأسباب تحقيقها.

ب- الانعكاسات على العاملين في الشركة

تفيد الإنترانت في عملية إدارة المشاريع الموزعة وتنفيذها، فإذا أرادت شركة ما أن تصمم منتجاً جديداً مع الاستفادة من الخبرات الموجودة في أقسامها المتباعدة جغرافياً، يجب عليها أن تؤمن عمليات الاتصال وتبادل المعلومات بين هذه الأقسام المختلفة حتى تتمكن من العمل معاً. ففي نهاية كل مرحلة يجب أن يُرسل كل قسمٍ التصاميم التي لديه إلى الباقين. هذا يعني أن يُرسل كل تلك المخططات الخاصة بالمشروع، بعد أن يحزمها جيداً، إلى ذلك القسم بالبريد العام، أو ببريد الشركة. إذن هنالك الكثير من العمل من أجل تحقيق عملية تبادل المعلومات بين الأقسام، كما أنها مكلفة.

في حال استخدام الشركة الإنترانت في إنجاز التصاميم، فيمكنها أن تجعل جميع الأقسام تعمل على نفس النسخة في نفس الوقت، كلٌ على الجزء الخاص به، لكن هذه الأجزاء تكون مجمعة معاً في بنية واحدة، ولا حاجة لتبادل التصاميم في كل مرحلة. على هذا النحو، توفر الشركة الجهد والمال، كما أنها توفر في الوقت أيضاً، فقد يكون اكتشاف أي خلل في التصميم أبكر في حالة استخدام الإنترانت، لأن بإمكان الجميع الوصول إلى أي جزء من تصميم المشروع (حسب السماحيات التي أعطتها الشركة).

في إحدى الشركات التي تعمل في مجال صناعة الطائرات، كانت توجد مجموعة من كبار خبراء تصميم الطائرات، لكن هؤلاء الخبراء كانوا موزعين على الفروع المختلفة، وكان كلٌ منهم يعمل على نموذج مختلف عن الآخرين. وقد واجهت الشركة مشكلةً تمثلت في أن هذه الفروع خرجت عن حدود المنافسة البناءة وبدأت الصراع فيما بينها. أرادت الشركة حل هذه المشكلات، والاستفادة من الخبراء جميعاً على نحوٍ أكثر فاعلية، بحيث يتشكل لديهم نوع من الحس الجماعي بالهدف المرجو، وهو تصميم طائرة جديدة. وقد حددت الشركة منذ البداية أن التركيز يجب أن يكون على العمل الجماعي المشترك في خدمة أهداف الشركة.

بنت الشركة إنترانت من المستوى الثالث، وقسمتها إلى مجموعة من الأقسام، كل قسم يخص فرعاً معيناً. بالطبع، مرت الإنترانت بمرحلة كان يجب فيها التخلص من العادات القديمة واكتساب

العادات الجديدة في العمل، وما أن تعود العاملون عليها، حتى بدؤوا باستخدام إمكاناتها، وبدأ مدراء الفروع يلتقون معاً من خلال المؤتمرات الفيديوية عبر الإنترانت، يتبادلون الخطط والأفكار والتجارب. كما بدأ العاملون باستخدام هذه التقنيات أيضاً وعقد اللقاءات التي تُسهم في تنمية خبراتهم.

تأثر فريق مهندسي المعلوميات بالوضع الجديد أيضاً، وبدؤوا هم أيضاً بالاستفادة منه. فعملوا على تلبية حاجات الشركة من البرمجيات التي تفيد في العمل الجماعي المشترك، وفي تنمية الإنترانت وإغنائها. فقاموا ببناء تطبيقات لتنظيم طريقة العمل المشترك، وأصبح بإمكان العاملين في المشاريع أن يختبروا نموذج الطائرة وهو على الورق من خلال هذه التطبيقات. كما أصبح بإمكانهم العمل معاً في بناء وتعديل النموذج دون أن يتداخل عمل أحدهم مع عمل الآخر.

إن المؤتمرات الفيديوية واحدة من المزايا الجيدة التي تُقدمها الإنترانت على المستوى الثالث. فاللقاءات وجهاً لوجه هي أفضل أنواع الاتصال بين الأفراد. إذ تقدم الإنترانت من خلال تطبيقات المؤتمرات الفيديوية إمكانية عقد مؤتمر بين فروع الشركة المتباعدة جغرافياً بحيث يرى كل شخص الآخر.

تحتاج تطبيقات الوسائط المتعددة إلى قسم كبير من موارد الإنترانت، وفي بعض الشبكات، لا يمكن استخدام هذه التطبيقات لأن عرض حزمة النقل غير كافٍ ليتحمل الحجم الكبير المطلوب نقله. إن إمكانية عقد المؤتمرات الفيديوية مرهونة بخصائص الإنترانت المستخدمة وسعة خطوط الاتصال فيها. كما أنها مكلفة جداً، ولكن قد يكون عقد مؤتمر على الإنترانت أقل كلفة من عقده في مقر الشركة مثلاً، فالشركة يجب أن تستقدم المحاضرين من مناطق بعيدة، كما يجب أن تدعو عدداً من الحضور وتتكفل بنفقتهم، وبهذا قد تكون التكلفة في صالح المؤتمر الفيديوي على الإنترانت.

6-3 انعكاسات الإنترانت على منهجية عمل الشركة وإدارتها

إن التغيرات التي تعصف بعالمنا المعاصر توحي بأننا على حدود نقطة فاصلة في تاريخ تنظيم المجتمع البشري، وهناك دلائل تشير إلى أننا على أبواب نقلة نموذجية أساسية حيث تحدث التغيرات في

التكنولوجيا والأعمال بسرعة يبدو معها العالم في فوضى مستقرة ! وقد أصبحت النظريات التقليدية في الإدارة والمؤسسات أقل قدرة على التوجيه إلى الأفعال المجدية، حيث تتغير جميع أنواع الأنشطة في الشكل والوظيفة والأهمية.

يبدو مصطلح "عصر المعلومات" الاسم المميز الأكثر شعبية للنظام الناشئ، وظاهرة الانتقال إلى المعلومات كمحرك أساسي هي السيطرة عند الحديث عن الحاضر والتنبؤ بالمستقبل والنظر في الماضي من وجهة نظر المعلومات المجازية.

إن الانفجار الذي نشأ في الاتصالات عند ظهور وسائط المطبوعات قد يكون من الأمور التي ساهمت في قيام الثورة الصناعية وما رافقها من تغيرات دراماتيكية في طريقة قيام الناس بأعمالهم، من حيث المهارات التي أصبحت مطلوبة والتغير في طريقة النظر إلى الأمور التي تؤلف قيمة الأشياء. والانفجار في الاتصالات الذي نشأ مع ظهور الإنترنت وتكنولوجيا الوب يَعِدُ بشمولية مماثلة في مجال رؤيته، وسنعرض فيما يلي كيف يمكن تؤثر مفاهيم الإنترانت على العمل وبيئة العمل في المستقبل.

تمكننا الإنترانت من الاتصال والإدارة بطرق لم نكن نقدر عليها من قبل، كما أنها تزودنا بتجربة حقيقية في مجال آلية عمل النظم الموزعة وكيفية إدارتها. وقد تؤدي الإنترانت إلى تغييرات في النموذج المؤسساتي، الأمر الذي يشجعنا على تعديل نظرتنا إلى كيفية إدارة المؤسسة، وكيفية تقويم العاملين فيها، وكيفية نمذجة المشاكل. لا تكمن النقلة الحاسمة في استخدام الإنترانت، وإنما في كيفية تقبل العاملين في حقل لإدارة والأعمال لها. ولأن الإنترانت هي ذلك العنصر المغير القوي، فإن فهم التضاربات الأساسية في النمذجة المؤسساتية يصبح أمراً لا بد منه.

وعموماً، فإن هناك نظرتين متضاربتين لرؤية المؤسسة وهما: المؤسسة كآلة هندسية إزاء المؤسسة كنظام عضوي ذاتي التكيف، أو بعبارة أخرى النظر إلى المؤسسة كخط للتجميع مقابل النظر إليها كبنية قابلة للتعلم. سنوضح فيما يلي وجهات النظر المختلفة في سبع ميزات للنقلة النموذجية التي أدت إليها الإنترانت وهي: الثقافة، الإدارة، التركيز، التنسيق، الأدوات، الاتصالات، التطوير.

6-3-1 الثقافة

يُقصد بثقافة المؤسسة طريقة التفكير المتبعة فيها وطرق تقويم العاملين التي تميزها عن غيرها من المؤسسات. تُستخدم الثقافة كقوة فاعلة في المؤسسات الصناعية التقليدية من خلال تخزين/ادخار المعلومات، بينما يجري التركيز في ثقافة الإنترانت على التشارك في المعلومات، إذ يجد المدراء الذين بنوا نجاحهم من خلال التحكم الحَذِر بالمعلومات وتحديد تدفقها صعوبةً في إدراك قيمة الإنترانت، وسيبحثون عن الأسباب والتقنيات للحد منها والتحكم بمضمونها. والمؤسسة التي تقيّم ثقافتها العاملين حسب قدرتهم على اتباع الروتين بدلاً من معرفتهم وخبرتهم، ولا تثق بأن يتصرف العاملون محلياً فيما يتعلق باهتمامات الشركة، يجب ألاّ تطبق الإنترانت !.

6-3-2 الإدارة

كانت القرارات تُؤخذ في المؤسسات التقليدية مركزياً، ومن ثم ترشح إلى أسفل هرم المدراء الموثوق بهم لكي يقوموا بإيصالها، وربما بتفسيرها والإشراف على تطبيقها. الإنترانت موزعة بشكل متأصّل، حيث تؤخذ قرارات التطبيق والإدارة محلياً. وتشكّل عملية اتخاذ القرار بطريقة موزعة قاعدة المؤسسة العضوية الذاتية التكيف، كما تقدم الإنترانت إمكانيات الاتصال لتنسيق إنتاج المؤسسة الموزعة لدعم هدف النشاطات المدارة.

6-3-3-التركيز

تركّز إدارة المعلومات في المؤسسات التقليدية على عمليات التطوير والتحسين والواجهات التخاطبية. في حين تركّز إدارة المعلومات بوجود الإنترانت، وبسبب طبيعتها الموزعة، على جمع وتبادل معلومات "الحالة". حيث تعود عملية اتخاذ القرار الموزعة إلى نظم كتليّة (Modular)، وبما أن العمليات ضمن الكتل المؤسساتية تعتبر أقل أهمية من حالة الإنتاج، فإن النجاح يصبح في هذه الحالة تابعاً للإدارة الشاملة لحالات المؤسسة وكتلها المستقلة وليس على العمليات التي تجري في كل كتلة.

6-3-4 التنسيق

يجري التنسيق في المؤسسات التقليدية من خلال البنية التنظيمية المتصلبة نوعاً ما. وفي بيئة الإنترانت التي تؤمن عمليات اتخاذ القرار الموزعة، فإن التنسيق يجري من خلال التشارك في معلومات الحالة التي تُجمع من قبل عناصر مؤتمتة وتُنظم حسب الحاجة. ولأن التنسيق يستند على المعلومات بدلاً من البنية التقريرية الثابتة (التنسيق عبر تبادل التقارير)، فإن فكرة المؤسسات الافتراضية والمرنة تصبح قابلة للتطبيق وعملية.

6-3-5 الأدوات

يجري التفاعل بين الأدوات في النماذج الحسابية التقليدية المبكرة عبر التخصص في منتجات وأدوات معينة. وتأتي قوة الإنترانت من حيادية المعايير المطلوبة من قبل البائعين. فهي لن تسمح للمؤسسات التي قامت بنقلة نموذجية كاملة بالتنويع في المنتجات والأدوات فحسب، ولكنها سوف تشجع على التنويع كضمانة المرونة المستقبلية.

6-3-6 الاتصالات

ثقافتنا المعلوماتية الحالية مبينة حول نموذج النشر بلا طائل !. حيث يجري إغراق المستخدم بالمعلومات التي تُرسل لسبب وحيد وهو أنه قد يحتاج إليها. الإنترانت هي نظام "أخذٍ وفق الحاجة" متأصّل، حيث يحصّل المستخدمون المعلومات على أساس حاجتهم الحالية لها بدلاً من إرسالها إليهم بلا سبب (بحجة هو أنهم قد يحتاجونها)، وقد يكون هذا المظهر هو الأكثر أهمية في النقلة النموذجية الحاصلة مع استخدام الإنترنت والتي تتطلب تغيرات في سلوك كلّ من مُرسلي المعلومات ومستخدميها.

6-3-7 التطوير

إن بيئات معالجة المعلومات الحالية تنقل مهمة إدارة ومعالجة المعلومات الإلكترونية من الخبراء الميدانيين إلى الخبراء التقنيين. بينما تؤمن الإنترانت الأدوات والبنية التحتية لإرجاع التحكم بعملية تطوير المعلومات إلى الخبراء الميدانيين. فبدلاً من النظر في تطبيقات مقترحة مثل مشاريع MIS (Management Information Systems) التطويرية، فإن النقلة النموذجية المتمثلة في الإنترانت من خلال تأمين أدوات البنية التحتية تسمح للخبراء الميدانيين بتطوير تطبيقاتهم بأنفسهم.

تشجع الإنترانت على انتشار آليات اتخاذ القرار الموزعة، والمؤسسات الكتلية، والاتصالات المفتوحة، والتطبيقات القائمة على استثمار معارف العاملين. هذه هي البديهيات التي تعتنقها علناً أغلب الإدارات الحالية. ويجب إدراك أن تحقيق هذه البديهيات ـ حتى مع وجود الإنترانت ـ قد يسبب بعض التحديات الصعبة في الإدارة والتي ستختبر مدى الالتزام بالطريق الذي جرى اختياره. وعندما يحدث ذلك، قد يكون من المفيد أن نتوقف ونطرح السؤال: "هل يتوجب علينا هَنْدَسَة كل مظهر من مظاهر المؤسسة كآلة أم أنّ عليها أن تستجيب ككيان قابل للتكيف ؟ أو بصيغة أخرى، هل نحتاج إلى خط للتجميع أم إلى مؤسسة قادرة على التعلم ؟".

الفصل السابع

مستقبل الإنترانت

سيتحدد مستقبل الإنترانت بالتوجهات التي ستتبلور في مجال الأعمال وبالتطور التكنولوجي اللاحق. فالإنترانت ستمكّن مستخدميها من ممارسة نشاطهم في الأعمال بفاعلية أكبر، لأن الاتصالات ستكون أكثر سرعة ودقةٍ. وبعد أن قمنا بعرض المعلومات النظرية والتقنية في مجال تصميم وبناء شبكات الإنترانت سنناقش في هذا الفصل مستقبل الإنترنت، ومدى تأثير الدراسات ومدراء أنظمة المعلومات والمستخدمين فيه.

يركّز هذا الفصل على التكنولوجيا والاهتمامات المختلفة التي ستحدد مصير الإنترانت، وتتمثل هذه الاهتمامات بالتقدم المتسارع في مجال الأعمال والميل نحو بناء اقتصاد عالمي يعتمد على المعلومات، وبالاتصالات المتقدمة والمتطورة، وظهور الشركات الافتراضية (سنقوم بتوضيح هذا المفهوم لاحقاً) التي تتدخل في إدارة أعمالها عدة مواقع (حتى من داخل المنازل)، وتوجه التطور التكنولوجي نحو البنى المفتوحة في تطوير التطبيقات، إضافةً إلى زيادة عرض الحزمة لنقل صور الفيديو المتحركة (الأفلام) والصوت الرقمي، وتطوير محركات بحث ذكية لتسهيل عمليات البحث والفهرسة، وتطوير تطبيقات زبون وحيدة مستقلة بحد ذاتها للحصول على مرونة وفائدة أكبر للمستخدمين. وفيما يلي سنتعرض بالتفصيل لكل من هذه التوجهات وأثرها في تحديد مستقبل الإنترانت.

1-7 التوجهات المستقبلية في مجال الأعمال

يرتبط تطور أنظمة الإنترنت والإنترانت ـ أو أيّ تكنولوجيا من شأنها مكاملة نظم المعلومات في مجال العمل ـ بالميول العامة في عالم الأعمال بدءاً من اعتبارات مصادر الدخل وحتى تقييم المستخدمين والمدراء لوظيفة الإنترانت. تهتم معظم الشركات حالياً بمفهوم جديد نسبياً هو "Data Mining"، وهذا المفهوم يرتكز أساساً على عملية التحليل للكمية الضخمة من المعلومات التي تكون مهملة غالباً أو مستخف بها، والتي تجمعت كنتيجة للتطور الطبيعي للأعمال مثل:

- بيانات المبيعات.
- قوائم البريد.
- معلومات الشكاوى عن المنتجات.

بجمع هذه المعلومات وإخضاعها لاختبارات عديدة والبحث عن مؤشرات حيوية جديدة وغير مكتشفة في دورة الإنتاج، يستطيع المنتجون إلقاء نظرة جيدة على:

- المناطق الضبابية في تكاليف الإنتاج.
- المنتجات نفسها.
- أسواق المنتجات.

كما تعتبر تكنولوجيا المعالجة الضمنية (Embedded Processing) من العوامل التي ستؤثر على بناء شبكات الإنترانت، وكذلك تطور أنظمة الاتصالات خلال العقد القادم، حيث تنخفض أسعار شرائح المعالجات على نحوٍ دراماتيكي، وأحد الاستخدامات الجديدة لها هو تضمين المعالجات في كل مكان: الهواتف الخليوية والمايكروويف وآلات الصودا، ويصبح من الممكن استخدام هذه المعالجات في جمع ومعالجة المعلومات، مما يعني جمع كمية أكبر من المعلومات، وهذه التكنولوجيا الجديدة ستولد الكثير من المعلومات حول الخدمات والمنتجات والتي يجب تحليلها وتخزينها، ومن دون توفر وسط عمل مثل الإنترانت ستجد الشركات نفسها تائهةً في بحر لا متناهٍ من المعلومات. إن هذه التكنولوجيا الجديدة تمكن الشركات من إرضاء زبائنها وزيادة أرباحها، ولنأخذ على سبيل المثال شركات الصودا.

تُجمع المعلومات حول معدل مبيعات الصودا من كافة أنحاء العالم لتخزينها ومعالجتها، وذلك من خلال شبكة إنترانت موصولة إلى شبكة واسعة النطاق ومنها إلى آلات البيع الآلية، مما يمكّن أي شخص في الشركة من الوصول إلى هذه المعلومات للقيام بالاستجابة المناسبة، مثل إرسال شحنات إضافية إلى بائع ما، وهكذا يمكننا القول أن آلة بيع الصودا استدعت الموزع على نحو ما عندما أصبحت فارغة، كما يمكن تحديد المناطق التي لا تحصل فيها مبيعات جيدة لتوجيه التسويق الإعلامي باتجاهها وبذل جهود إضافية فيها.

لقد شكلت الإنترانت طريقة ثورية في الاتصالات باعتبارها مصدراً للمعلومات وقناة للتوزيع، لكن الميزة المهمة في الإنترانت أنها توفر نفاذاً عادلاً لأي شخص في الشركة للحصول على أي معلومة.

وعلى كل شركة ترغب في أن تجني منفعةً كبيرة من التطورات الجديدة في عالم الاتصالات المتمثلة بالإنترانت، أن تبذل جهوداً واعية لخلق الجو الملائم الذي صممت الإنترانت لتزدهر فيه. وبالرغم من أن هذه المهمة ليست سهلة، إلا أنها ضرورية لكل شركة ترغب في زيادة إمكانيات الاتصالات فيها إلى حدها الأعظمي.

كما يجب على الشركات أن تقوض البناء الهرمي المبنية عليه لأن قوة الإنترانت تكمن في أن أي عامل يستطيع الوصول مباشرةً إلى المعلومات ومعالجتها، الأمر الذي سيزيد كثيراً من عدد العاملين الذين يملكون المعلومة والذين عليهم استخدامها لاتخاذ القرارات.

ستختصر الشركة الوقت وتوفر في النفقات إذا قامت بتقويض البناء الهرمي، ويتم ذلك عندما تدعم وتسمح للعاملين باتخاذ القرارات على مسؤولياتهم، ويجب أن نتذكر أن هؤلاء العاملين مختارون بدقة وعناية لإدارة موارد الشركة وحل مشاكلها وتطوير مشاريعها.

7-1-1 إعادة تشكيل قوة العمل

إن ظهور الإنترانت وبعض التطورات التكنولوجية الأخرى سيلغي بعض الوظائف التي يقوم بها عاملو الشركة، وخاصة هؤلاء الذين يقومون "برزم المعلومات"، مثل إدخال المعلومات، وإدارة السجلات،

والمراقبة على المستويات الدنيا، وحفظ الأوراق في الملفات والقيام بعمليات البحث الأساسية. يقابل هذا الانخفاض في قوة العمل في أحد قطاعات الشركة ازديادٌ في قطاع آخر، ويشتمل ذلك على العاملين الذين يعملون على استثمار موارد الإنترانت في أعمالهم اليومية، وكذلك العاملين الذين يملكون الأرضية المناسبة لمواكبة التطور التكنولوجي الحالي والمستقبلي.

يجب أن نذكر هنا أنه ليس بإمكان الحواسيب اتخاذ سوى القرارات البسيطة، كما أنه لن يكون بإمكانها في المستقبل القريب اتخاذ القرارات المتقدمة، لذلك يجب على العاملين عدم النظر إلى الإنترانت وأنظمة المعلومات الأخرى على أنها ستحل مكان صانعي القرار.

وبنظرة أكثر شمولية إلى الإنترانت فإنها ستزيد من الإنتاجية وتخدم الاقتصاد العام عن طريق محاكاة شاملة للتجارة، والتخطيط المتطور للتسويق وذلك بالاعتماد على تحليل توجّهات السوق عن طريق الحاسوب.

7-1-2 مجال اتصالات الأعمال

إن تكنولوجيا الإنترانت قللت من أهمية الحدود الجغرافية في الاقتصاد العالمي، فيمكن إرسال معلومة إلى إي شخص في بلد آخر (عبر البريد الإلكتروني مثلاً) بالسهولة نفسها التي نرسل بها هذه المعلومة إلى شخص في المبنى نفسه. ومن الأمور الأكثر فاعلية إمكانية الاتصال بالمدراء في مختلف المواقع كاسرين الشكل التقليدي في الشركات الذي يقضي بأن تكون الاتصالات في الموقع الفيزيائي نفسه لأن هذا الشكل لم يعد متوافقاً مع تكنولوجيا الإنترانت. فقد أصبح بإمكان الأشخاص والشركات الاتصال بغض النظر عن القيود الجغرافية أو السياسية، وهذا يتلاءم مع الاتجاه نحو عولمة التجارة والتخصص في العمل، كما هي الحال في الشركات الافتراضية التي سنشرحها لاحقاً.

أصبحت الإنترانت ومصادرها المختلفة تمتلك نفس أهمية الشركة ذات المكاتب القائمة في مبنى واحد، إذ أصبح بإمكانها وصل البعيدين منهم بعضهم ببعض، وتسمح للقريبين منهم، بالقيام بأعمالهم بطريقة مختلفة: ربما من البيت أو حتى من الطائرة. على سبيل المثال تستطيع شركة ما تغيير

استراتيجيتها تغييراً كاملاً لأن أنظمة الاتصال لديها تضمن منهجية جديدة في تشارك العمل، كما تستطيع اختصار عدد مكاتبها إلى ثلث عددها السابق موفرةً في النقود والمكان.

وبدلاً من أن يكون لكل شخص مكتب دائم ويشغل مكاناً في مبنى ما، فإنه بمقدور الناس اليومَ العمل من منازلهم أو وهم في الطريق. يشار إلى هذا النوع من نظام العمل بالـ "Hoteling" حيث يدار المكتب الرئيسي للشركة بطريقة مشابهة لإدارة الفندق.

كما توفر الإنترانت حلاً مناسباً للأشخاص الذين لا يرغبون بالتواجد فعلياً داخل مكتب واحد خلال الفترة الرسمية للعمل (من خمس إلى تسع ساعات)، وهذه الطريقة في العمل توفر على الشركة المال وأجرة المكاتب والمعدات وغيرها، وتوفر على الأشخاص بعض المال اللازم للملابس والغذاء والانتقال وما إلى ذلك من نفقات يفرضها العمل، وتسمح لهم بقضاء وقت أكثر مع عائلاتهم مما يجعلهم أكثر قدرة على الإنتاج.

2-7 اقتصاد المعلومات

العامل الأكثر أهميةً بالنسبة لشخص أو شركة في عالم الأعمال هذه الأيام هو المعلومات، سواء كانت على شكل معطيات عامة أو محددة أو على شكل تقارير تحليلية، وسنرى باستمرار التطور المطرد لاقتصاد المعلومات الذي سيكون المحرّض الأساسي لصفقات العمل الحديثة، حتى أن شراء وبيع المعلومات ينمو لدرجة منافسته للتجارة التقليدية (تبادل المنتجات التقليدية). والمعلومات هي التي تحدّد القدرة التنافسية لشركة مقارنةً بأخرى، فهي تمكّن الشركة من فهم حالة السوق والقيام بالاستجابة المناسبة في حالة الأزمات المالية أو التغير في احتياجات السوق. وتحاول الشركات باستمرار تحسين مواقعها ليكون لها نصيب في النمو والازدهار المستقبلي وذلك ببذل الجهد في جمع المعلومات وتحليلها لمواجهة المنافسة.

بدأ عدد متنامٍ من رجال الأعمال بإدراك أهمية المعلومات في مجال الأعمال وأخذوا يكتشفون طرقاً جديدة فعالة في جمع المعلومات وتحليلها ومعالجتها لينتقلوا بعدها لإجراء تغييرات أساسية في

علاقتهم بالزبائن من جهة وبالسوق من جهة أخرى. ولقد ساهمت الإنترانت والتكنولوجيا المرافقة لها بإعطاء فرص متساوية للجميع، حيث أن مصادر المعلومات كانت فيما مضى حكرا على الشركات الضخمة وكبار رجال الأعمال.

يمكن شراء المعلومات مثلا من ملقمات الأخبار مباشرة مثل وكالات الأنباء التقليدية كوكالة رويتر أو AP أو من الأخبار المنشورة على الإنترنت مثل موقع الشركة Individual, Inc. (www.individual.com) أو من PointCast Network (www.pointcast.com). على سبيل المثال يمكن أن تطلب الشركة من مكتب خدمات معين تزويدها بالأخبار، مقابل مبلغ معين، حول مواضيع معينة، وذلك بإرسالها مباشرة إلى شبكة الإنترانت حيث يستطيع كل العاملين الاطلاع عليها الأخبار دون الحاجة للاشتراك في الصحف والمجلات مما يؤدي التوفير في المال والوقت.

توجد بالطبع تكنولوجيا متممة للتأكد من نجاح الإنترانت في الأعمال مثل تقنية الترشيح التي تقوم بفصل الأخبار الهامة عن الأخبار التافهة بناء على احتياجات العاملين خصوصا و الشركة عموما.

تستطيع ملقمات الأخبار تأمين معلومات هامة من داخل الشركة، إضافة إلى المعلومات التي تؤمنها من خارجها، مثلا من المكن رصد حركة المبيعات في كل لحظة وتأمينها للعاملين. تسمح هذه التكنولوجيا للناس أن يروا آنيا حركة المبيعات لكامل الشركة أو لمناطق محددة في مجال نشاط الشركة، وترتبط أعمال بيع المعلومات بتطور اقتصاد المعلومات وتسارع قرارات الأعمال، حيث تمتلك المعلومات أهمية لحظية كبيرة، وهي عرضة لأن تصبح عديمة القيمة إذا لم تصل في الوقت المناسب وبطريقة فعالة.

لذلك يجب على الشركات التي تبيع المعلومات الحصول عليها بأسرع ما يمكن اعتمادا على التكنولوجيا أو على الجهود الشخصية. وكمثال جيد على القيمة اللحظية للمعلومات نأخذ حالة الخدمات السلكية:

مراسلة صحفية لمؤسسة مسؤولة عن الأخبار في هونغ كونغ تتحدث اللغة الصينية والإنكليزية ويجب عليها أن تقوم بتغطية مؤتمر صحفي في هونغ كونغ حيث اللغة الصينية هي اللغة الرسمية المعتمدة،

تتمثل عملية التغطية بأن تُترجم هذه المراسلة أحداث المؤتمر في الزمن الحقيقي عبر هاتف خليوي، ويقوم الشخص في الطرف الآخر من الخط بكتابة المعلومات الواردة لإرسالها مباشرة عبر الخدمات السلكية من دون إضاعة الوقت في أخذ الملاحظات وتدوينها ومن ثم إرسالها بالفاكس. إن هذه الطريقة المُحكمة و"المضغوطة" في العمل هي التي ستزيد من احتمال نجاح رجال الأعمال، كما أنها ستميز بين الناجحين والخاسرين في مجال المعلوماتية.

إن معظم المشتركين بمثل الخدمة السابقة هم أناس يحتاجون للحصول على المعلومة فوراً، كالتجار الذين تعتمد تجارتهم على هذه المعلومات، وأي وقت إضافي يُصرف في كتابة وترجمة التقرير وإرساله عبر الفاكس قد يشكل حرجاً. في الواقع إذا نظرنا إلى القضية من وجهة نظر أخرى: مصادر المعلومات متاحة للجميع في نفس اللحظة، سيبدو الوقت كما لو أنه هو المنتج الذي تبيعه الشركة، وبالتالي يجب الاعتماد على تكنولوجيا الإنترانت للاستمرار في المنافسة على نحو فعّال.

ستكون الشركات التي تستخدم تكنولوجيا الإنترانت على نحو فعّال أكثر قدرة على الاستجابة للتغيرات، وعلى اتخاذ قرارات سريعة مبنية على معلومات جيدة، وإنتاج منتجات ذات جودة أعلى بسهولة أكبر وتسليمها للزبون بسرعة وبتكلفة أقل. إن الشركات الكبيرة قادرة على شراء التكنولوجيا أسرع من غيرها، وبالتالي تستطيع تحقيق فائدة أكبر، لكن من جهة أخرى تستطيع الشركات الصغيرة أن تتأقلم بسهولة مع أي تكنولوجيا جديدة على عكس الشركات الكبيرة التي تميل إلى لتحرك ببطء، أي يمكن للشركات الصغيرة تحقيق الفائدة أيضاً.

وعلى كل حال فإن تكنولوجيا الإنترانت لا تساعد الشركات الكبيرة والصغيرة فقط، بل تقدّم فوائد حقيقية لأي شركة تدرك أهمية أنظمة المعلومات المفتوحة وإدارة الاتصالات.

7-2-1 المؤسسات التعاونية التخيلية (أو الافتراضية)

أحد الاتجاهات في عالم الأعمال والذي تساعد عليه أنظمة الإنترانت هو ظهور ما يسمى بالمؤسسات التخيلية. تتشكل المؤسسة التعاونية التخيلية عندما تعمل عدة مؤسسات ـ ذات اختصاصات مختلفة

غالباً وفي مناطق جغرافية متنوعة ـ سوية ككيان واحد لخدمة متطلبات زبائن خاصين بمجموعة المؤسسات هذه، أو لدعم جهود البحث المشتركة. يمكن للمؤسسات التخيلية باستخدام الإنترانت أن تعمل معاً بتقارب أكبر، وأن تنسق فيما بينها تنسيقاً أفضل، وأن تنافس كشركة واحدة. وتأتي تسمية هذه المؤسسات بالافتراضية من كونها تملك بنية مادية محدودة أو معدومة.

7-2-2 الاقتصاد العالمي

بما أن القيود الدولية في مجال الأعمال قد تقلصّت إلى حدّ كبير وقلت الحواجز التجارية فإن نشاط الشركات المحلية يتحول من جداول للأعمال على المستوى القومي إلى استراتيجيات عالمية، وتتطلع الشركات إلى زبائن في مختلف أنحاء العالم وتقدّر المنتجات والخدمات التي يمكن أن تقدمها لهؤلاء الزبائن. وتقوم الشركات، في سعيها نحو الاقتصاد العالمي، بكل شيء ابتداءً من كتابة البرمجيات بمختلف اللغات إلى أمْرَكَة الثقافات الأخرى بالمنتجات الأمريكية أو حتى بتصدير "الذكاء" التسويقي الأمريكي.

على كل حال، للحصول على علاقات بيع ناجحة على مستوى عالمي يجب البدء بفهم الميول التي توجه الثقافات وبيئة الأعمال في البلد المعني، وتلعب الإنترانت دوراً نموذجياً في تتبع القضايا العالمية نظراً لكونها ترفع من سوية نفاذ المؤسسات إلى المعلومات.

7-2-3 الاتصال عن بعد والـ Hoteling

سوف تستمر الاتصالات عن بعد في المستقبل، وفي بعض الحالات سوف يحل مفهوم الـ Hoteling محل كافة الإجراءات المكتبية النمطية، نذكّر بأن مفهوم الـ Hoteling يعني أن يحتل العاملون مكاناً فيزيائياً عند حاجتهم لمقابلة زملائهم أو زبائن الشركة حصراً، وفيما عدا ذلك فإنهم يتواصلون مع العمل عبر الإنترانت بغض النظر عن المكان الفيزيائي الذي يعملون فيه والذي قد يكون المنزل أو غرف الفنادق. ففي أغلب الحالات تلغي الإنترانت الحاجة إلى التخزين الورقي في المكاتب، حيث

ينوب التخزين الإلكتروني عن ضرورة الوصول الفيزيائي إلى الملفات المخزنة في موقع العمل، الأمر الذي يؤدي بدوره إلى عدم ضرورة البقاء بقرب هذه الملفات للقيام بالعمل.

وعلى نحوٍ مماثل، فإن الاتصال عن بعد من المنزل مثلاً يسمح بالوصول إلى كل المعلومات المخزنة على الإنترانت مما يلغي الزمن الضائع بين العاملين في المكاتب والعاملين من المنزل، وستستمر الإنترانت بفتح أبواب جديدة أمام تعاون العاملين مما يؤدي إلى التعاون الكامل بين كافة العاملين بغض النظر عن مكان وجودهم.

7-2-4 الاعتماد على المصادر الخارجية

أينما وُجد تقلصٌ في الحجم التعاوني (إنقاص عدد العاملين) ولا مركزية في الحكومة وازديادٌ في سيطرة الحاسوب، فإن الكثير من الأعمال سوف تتجه نحو الاعتماد على المصادر الخارجية، الأمر الذي يتمثل بالاعتماد على مستشارين ومتعاقدين ـ مؤقتين أو دائمين ـ لتحقيق عمل معين بدلاً من الاعتماد على عاملين بدوام كامل لتحقيق العمل نفسه ؛ مما يعني أن الشركات لن تضطر إلى دفع مستحقات الضمان الصحي أو أجور التقاعد أو حتى بعض الضرائب التي تستحق على العاملين. فغالباً ما يؤدي الاعتماد على مصادر خارجية إلى توفيرٍ ذي أهمية، وهنا تأتي أهمية الإنترانت في تسهيل عملية تأمين المصادر الخارجية من خلال كونها مركزاً لمصادر المعلومات الأساسية للشركة أو المشروع، مختصرة عدد الساعات التي قد يقضيها عامل ما في مناقشة أحد الاستشاريين أو المتعاقدين قبل البدء بتنفيذ مهامه.

حتى ولو كانت المؤسسة لا تخطط إلى تقليص عدد العاملين فيها، فإن الحاجة إلى العاملين الجدد مستمرة دائماً وذلك عندما يستقيل أحد العاملين أو يرتفع إلى مركز وظيفي أعلى، وبوجود الإنترانت يمكن توفير الكثير من مصاريف التدريب وإعادة التأهيل. يمكن توضيح هذه النقطة بالمثال التالي: لنفترض أن أحد العاملين سوف يترك العمل في أحد المشاريع الحالية في الشركة، بالتالي فإن جميع الخبرات والمعلومات ستذهب بذهاب هذا العامل، وغالباً ما تكون الملاحظات التي قد يتركها هذا

العامل أو الملفات على الحاسوب لا تعني شيئاً إلا لهذا العامل، وفي الإنترانت جيدة التصميم يجب أن يتوفر للمستخدمين الجدد الذين يستخدمونها لأول مرة خط سير جذاب وفي مثل هذه الإنترانت سوف يصبح الوصول إلى معلومات أعمال المشاريع المخزنة متاحاً وفق طرق معيارية، ولن يعود من الضروري تواجد العامل السابق للإجابة عن الأسئلة وتفسير الغاية من كافة الملفات التي كان يعمل عليها ؛ وهذا يعني عبثية أن يقوم الأفراد ببناء أجزاء شخصية من المعلومات لا يفهمها ولا يصل إليها أحد غيرهم، وبالطبع فإن الأمور التي تصعب من استخدام الإنترانت تجعلها غير ذات قيمة أيضاً، فالإنترانت هي كيان غير منتظم وإذا لم تستخدم وتحدّث فإنها سوف تموت، فهي تشيّد مركزاً للمعلومات يسهّل العمل ويقلل من تأثير الانحرافات في بيئة العلاقات الشخصية والتعاونية.

7-3 الآفاق التكنولوجية

التوجهات التكنولوجية التي ستؤثر في الإنترانت وتتأثر بها متنوعة ومختلفة مثل المعايير المفتوحة، وعرض حزمة النقل، والاتصالات اللاسلكية، وتطبيقات الزبون الوحيدة، والتكامل المتزايد في التطبيقات، والبريد الصوتي وبوابات الفاكس، والعناصر الذكية، وغيرها من التطبيقات الجديدة. في الفقرات القادمة سنغطي بعض هذه المواضيع هادفين إلى تزويد القارئ بنظرة شاملة للاتجاهات الحديثة في تكنولوجيا الإنترانت والإمكانيات التي تلوح في الأفق.

7-3-1 المعايير المفتوحة

أحد التوجّهات القوية في بناء الإنترانت هو الاتجاه نحو المعايير المفتوحة، والمعروفة أيضاً بالبروتوكولات المفتوحة أو البنى المفتوحة.

تهدف المعايير المفتوحة إلى إتاحة الاتصالات بسهولة وسلاسة بين مختلف التطبيقات التعاونية، وإلى تمكين هذه التطبيقات من التكامل بعضها مع بعض بسهولة وفعالية. وتسمح الإنترانت بأن تُكتب كل

البرمجيات باستخدام المعايير المفتوحة، ولكن قد لا يكون هذا خيار كل الشركات ـ في بعض الأحيان لأسباب أمنية ـ بسبب النقص في المعلومات المفيدة حول هذا الأمر.

تسمح المعايير المفتوحة ببناء الإنترانت على أسس معيارية مما يعني أن جميع التطبيقات ستتخاطب بلغة واحدة، وأهم المعايير المفتوحة هو TCP/IP الذي تستخدمه كل شبكات الإنترانت بالتعريف، بغض النظر عن اللغة الخاصة التي تنطبق على تطبيق معين. فمثلا يعتمد تطبيق Microsoft Word على معيار مغلق خاص بالشركة المنتجة، لأن مستندات Microsoft Word لا يمكن تحريرها إلا باستخدام هذا التطبيق، ويمكن وجود بعض البرمجيات التي تسمح بقراءة مستندات Microsoft Word ولكن عن طريق الالتفاف حول الموضوع ليصبح بالإمكان قراءة هذه المستندات على بيئات لا تتناسب مع البيئة الأصلية لها.

إن النقص الموجود في المعايير المفتوحة هو أحد الهواجس الرئيسية لمولي شبكات الإنترانت الذين لا يرغبون حتما بإنفاق المبالغ الطائلة لبناء شبكة إنترانت، ليجدوا فيما بعد أن التطبيقات المستقبلية مصممة بلغات مختلفة وبالتالي غير متوافقة مع الأنظمة الحالية. وعلى الرغم من أن المعايير المفتوحة ليست معايير مطلقة إلا أنها ضمانة أكبر للوظائف المستقبلية المتوقعة ضمن التقلب الموجود في تطور الصناعة البرمجية، والإنترانت بحد ذاتها تستخدم كثيرا معايير مفتوحة قوية، وبالطبع فإن قوة الإنترانت وشعبيتها تأتي من حقيقة كونها تستخدم مثل هذه المعايير.

كمثال على اعتماد المعايير المغلقة لنأخذ مؤسسة تستخدم Microsoft Word للمعالجة النصية، وLotus لمعالجة الجداول التجارية، وInformix كنظام قواعد معطيات ؛ فجميع هذه التطبيقات غير متوافقة فيما بينها، إذ يستحيل طباعة الرسائل من Informix باستخدام Microsoft Word إلا إذا قامت الشركة ببناء تطبيقات برمجية خاصة للوصل بين هذه التطبيقات، وبالتالي يجب الحذر باختيار التطبيقات التي قد تكون حرجة بالنسبة لمهام الشركة.

7-3-2 عرض حزمة النقل

قد تكون هذه التكنولوجيا هي الأكثر سرعة في التطور، ففي عام 1994 كانت أغلب الموديمات تعمل بسرعة نقل 2400Bps أو 9600BpsK وبعد سنة تقريباً أصبحت سرعات الموديمات 28000Bps و حالياً بلغت سرعتها 56000Bps، مما يعني أن الاتصالات عن بعد أصبحت خياراً أكثر قابلية للتطبيق في المجال التعاوني، والأبحاث الحالية تؤدي إلى قفزات كبيرة في السرعات المكن الوصول إليها سواء في حالة الموديمات السلكية أو خطوط ISDN أو الموديمات الرقمية.

وعلى الرغم من الآمال المعقودة على تطوّر سرعة الموديمات السلكية إلا أن أسعار البرمجيات والمكونات الفيزيائية الخاصتين بتقنية النقل باستخدام ISDN تتناقص بسرعة، وبالتالي فإنها تزداد انتشاراً، ومن الممكن أن تظهر تكنولوجيا جديدة تقدم سرعات أكبر من تلك التي تقدمها تكنولوجيا ISDN، وقد تكون النقلة التالية هي الوصول إلى سرعة 10MBps (كما هي الحال في سرعات شبكة الإثرنت) وستصبح تطبيقات الزمن الحقيقي، مثل المؤتمر الفيديوي والمؤتمر الصوتي وتطبيقات نقل الفيديو عن بعد، ممكنةً وأكثر عمليّة.

وقد تسود إحدى الطريقتين: ISDN أو الموديمات السلكية على الأخرى، وفي كلتا الحالتين سوف يصبح نقل مختلف أنواع المعطيات أسهل في المستقبل القريب، وفي جميع الأحوال فإن التصميم الناجح للإنترانت يجب أن يتوافق مع أبطأ سرعة نفاذ إليها من قبل المستخدمين، حيث أن هذا الأمر محكوماً بسرعة النقل عبر خطوط الهاتف.

ولكن هذه السرعات ستتغير في المستقبل القريب لتصبح السرعة 10MBps من المعايير النظامية، مما سيؤدي إلى إتاحة الاتصالات من رتبة 100MBps لتصبح بدورها نظامية أيضاً. وعند تصميم الإنترانت آخذين بعين الاعتبار عرض حزمة النقل يجب تكوين صورة صحيحة عن احتمالات النمو على أساس تعدد الاتجاهات والتكنولوجيا.

أما بالنسبة للاتصالات داخل الشبكة المحلية فإنها تتمتع بعرض حزمة كبير (10/100MBps)، وإذا كانت عمليات النفاذ إلى الإنترانت تجري عبر الشبكة المحلية مباشرة فيمكن إدخال التطبيقات

المتعددة الوسائط في تصميم الإنترانت بسهولة، حيث أن سرعة النقل في الشبكة المحلية تدعم أي تطبيق يتطلب عرض حزمة نقل كبيراً.

وغالباً ما يجري النفاذ إلى الإنترانت عبر الموديمات مما سيؤثر بوضوح على التطبيقات العاملة عليها لسنوات عديدة، فالمؤتمر الفيديوي مستحيل، وكذلك الأمر بالنسبة إلى المؤتمر الصوتي. كما يُعتبر من المكلف اليوم ربط المواقع البعيدة بشيء أقوى من الموديمات التقليدية، إلا أن الأسعار تميل إلى التناقص بسبب تزايد مقدرات خطوط النقل ورغبة مزودي خدمة الإنترنت ISP في تحريك قاعدة السوق.

وتسعى شركات الهاتف حالياً إلى تقديم عرض حزمة نقل أكبر، وتتطور العلاقة بين هذه الشركات ومزودي خدمة الإنترنت بصورة متكاملة نوعاً ما، حيث أن شركات الهواتف لم تأخذ أمر الإنترنت على محمل الجد في البداية، ولكنها تهتم بها الآن أكثر، وسوف يزداد التعاون والتشارك في مجال الاتصالات، فشركات الهاتف وشركات الكابلات والخدمات اللاسلكية ومزودو خدمة الإنترنت يرغبون في السيطرة على السوق في مجال الوصل إلى الإنترنت.

وأمام إغراءات تناقص أسعار الوصلات مع الإنترنت (التي ستصبح أكثر سرعة في النقل)، فقد يصبح من غير الممكن تجنب الاختناقات في الإنترنت، مما سيؤثر على الأعمال والمستخدمين الأفراد. وعلى الرغم من أن حدوث مثل هذا الأمر سيؤدي إلى خطر حقيقي إلا أن هناك جانباً آخر من التطور التكنولوجي، وهو التطور المتسارع في تقنيات التوجيه السريعة مما قد يخفف من أثر هذا الخطر. وعلى كل حال إذا شكلت الاختناقات مشكلة في الإنترنت فهناك حل منطقي مطروح من قبل العاملين في الاقتصاد والعلماء ويتمثل بزيادة الرسوم على استخدام الإنترنت، مما يقضي بأنه كلما زاد عرض الخدمة المستهلك كلما ازداد المبلغ المدفوع. ولكن هذا الحل سيكون صعب التحقيق لسببين:

- لأن الإنترنت ذات بنية لامركزية تماماً، وستخفق أي شركة أو مدينة أو دولة في فرض هذه الرسوم بدون اعتراض المستخدمين والجهات الأخرى.

- لأن مراقبة المعطيات المنقولة ومن ثم جمعها ومعالجتها وحساب الفاتورة (وهو لا يتم بالسهولة التي تتم بها حساب فاتورة الخدمات البعيدة) سوف تكون مهمة صعبة التحقيق، وعلى كل حال فإن هذا الأمر لن يحدث قريباً.

7-3-3 الاتصالات اللاسلكية

تتناقص أسعار الاتصالات اللاسلكية مع تزايد قوتها، وهذا الاتجاه في تطوّر التكنولوجيا لا يبدو أنه قد يتغير نحو الأسوأ، وحالياً وكما هو متوقع في المستقبل فإن الاتصالات اللاسلكية هي أبطأ أنواع الاتصالات وكذلك الأمر بالنسبة لنقاط الوصل بين الشبكات التي تعتمد على الوصل اللاسلكي، وبالنسبة للمستخدمين فإن أبطأ سرعة في النفاذ إلى الإنترنت تكون عند استخدام الموديمات اللاسلكية، وإن قبول الحواسيب المسماة بـ "Palm-top"، والتي سنتحدث عنها لاحقاً، متوقف على نجاح الاتصالات اللاسلكية في إثبات وجودها، وهذا سيؤثر بالتأكيد على مرونة استخدام الإنترانت في المستقبل، وعندما يصبح بالإمكان استخدام النفاذ اللاسلكي عن بعد فإن الإقدام على استثمار الإنترانت سيتزايد زيادةً ملحوظة.

7-3-4 برنامج الزبون الوحيد

لا نعرف من هو الذي أتى بهذه الفكرة، وهي تقضي بأن يكون هناك برنامج زبون وحيد يقوم بكافة الخدمات، حيث تتنافس شركتا Microsoft و Netscape على احتلال المكانة الأولى وقد قررت كل من هاتين الشركتين على جمع وظائف المستعرض وبرامج أخرى مثل برنامج إدارة الملفات المحلية، وخدمة نقل الملفات باستخدام FTP، وخدمة البريد الإلكتروني وتطبيقات أخرى في برنامج واحد ضمن واجهة تخاطبية مشتركة. كما أن تقنية الزبون الوحيد استخدمت في الإصدار التجريبي لبرنامج Microsoft News&Mail الذي يعمل في بيئة Windows 95 و Windows NT، وكذلك في برنامج Netscape 3.0، وبدا أن الفكرة قد تكون جيدة حيث أصبح التعامل مع الأعمال اليومية يجري عبر

برنامج وحيد بدلاً من الاعتماد على العديد من التطبيقات المختلفة، وبالطبع يتفق العديد من المستخدمين على أن تطبيق الزبون الوحيد سوف يكون حلاً نموذجياً على الأقل من ناحية التكلفة، والتي ستكون أقل من تكلفة شراء مجموعة من التطبيقات المختلفة، كما أن تعلُّم التعامل مع هذا البرنامج يتطلب وقتاً وجهداً أقل، ولكن فكرة وجود تطبيق وحيد تعاني من العديد من السلبيات:

- لأن بناء الإنترانت بالاعتماد على تطبيق زبون وحيد يعتمد على الشركة المصنعة يعتبر مناقضاً لما تحدثنا عنه بخصوص المعايير المفتوحة، فمن المحتمل أن تتوقف الشركة المصنعة عن إصدار نسخ حديثة من البرنامج أو قد تتوقف عن دعم المنتج نهائياً.
- لأنه عندما كانت الشركات تحاول جمع عدد كبير من الوظائف المستقلة في منتج واحد، فإن هذا المنتج الناتج غالباً ما يكون عديم النفع. والمحاولة الوحيدة الناجحة في هذا المضمار كانت في إنتاج سكين الجيش السويسري (Swiss Army Knife) المعروفة بتعدد وظائفها !. وفي صناعة البرمجيات والحواسيب يمكن أن نذكر بعض الآلات التي أنتجتها عدة شركات والتي تقوم بمهام الطباعة والفاكس وماسح الصور والآلة الناسخة، وعلى الرغم من أن المنتج كان عملياً ورخيصاً، فإن هذه الآلات كانت توفر في المكان الذي تشغله على حساب الدقة وأمور أخرى، واتضح بأنها لم تكن فكرة جيدة. وعلى كل الأحوال فإن الفكرة تستحق المحاولة وقد تظهر أنظمة زبون وحيدة ناجحة في المستقبل القريب ولكن الاعتماد على هذه التطبيقات يجب أن يجري بكثير من الحذر.

7-3-5 البريد الصوتي وبوابات الفاكس

لقد غيّر دخول أنظمة الحواسيب الشخصية الإجراءات المكتبية اليومية وتقاليدها جذرياً ابتداءً من السياسات المتبعة إلى الثقافة التعاونية وانتهاءً برضى العاملين. على هذا النحو سيتابع هذا التوجه منحاه في جمع التقنيات الوسيطة التي لا زالت حاضرة منذ بعض الوقت بما فيها الصوت وآلات الفاكس، ومن المهم معرفة أن هذا الميل ليس مجرد تحديث في التكنولوجيا، بل يمكن وصفه على أنه

نقلة نوعية في ساحة العمل المكتبية، وهذا ما سيتبلور طبعاً خلال فترة زمنية طويلة نوعاً ما. لكن حتى ذلك الحين فإننا سوف نلحظ تحسناً وتغيراً تدريجياً ولكن متماسكاً أيضاً بالنسبة إلى كل من النظامين (البريد الصوتي والفاكس) بحد ذاتهما، وكذلك بالنسبة لدورهما في بيئة متقدمة مهنياً.

وفي المدى القصير يمكن أن تصبح أنظمة البريد الإلكتروني وبوابات الفاكس متكاملةً في شبكات الاتصالات المحلية والإنترانت، ليصبح بالإمكان النفاذ داخلياً إلى الفاكسات إضافةً إلى النفاذ عن بعد، وباستمرار التطوّر في هذا الاتجاه فإن جزءاً من، وربما كل، وظيفة مخدّمات هذه التطبيقات ستصبح جزءاً لا يتجزأ من تخديم المعلومات التي ستكون خاصة بالإنترانت.

7-3-6 العناصر الذكية

أحد الأمور التي ستحدث في الإنترانت هي تطور عناصر ذكية عاملة فعلياً، وظهور تطبيقات يمكن إعطاؤها وسائط أساسية لتقوم بعمليات البحث وتوليد تطبيقات CGI والجدولة، لتعطي في النهاية منتجاً أولياً يراجعه أو يقبله مدير الشبكة. إن الإنترنت مصدر ضخم للمعلومات ويمكن تشبيهها بمكتبة كبيرة ولكنها لا تملك فهارسَ، ومن ثم لا يمكن لأي مستخدم إيجاد كل شيء في هذه المكتبة في جلسة عمل واحدة، ولكن ببناء عناصر ذكية يمكننا القيام بذلك، وفي المستقبل وبتطور معالجات الاستفسارات باللغات الطبيعية وتقنيات أخرى متممة، إضافةً إلى أنظمة Dewey Decimal-Sequa المعيارية من أجل الشبكات، يصبح من المتوقع ظهور تقنيات بحث أسرع وأكثر قوة فعالية.

وعلى سبيل المثال إذا كانت إحدى الشركات تدير رأس مال استثماري في الصناعة في بلد ما، فقد ترغب في امتلاك أحد العناصر الذكية لمراقبة مصادر الأخبار بحيث يجوب هذا العنصر الشبكة بحثاً عن الأخبار المالية الخاصة بالبلد المحدد، ومن ثم يخزن الأخبار ذات الصلة آلياً في الأماكن المناسبة على الإنترانت الخاصة بالشركة، كما قد يجري إظهار الأخبار المتعلقة ببضائع الشركة التجارية مباشرةً على شاشة مدراء الشركة، الأمر الذي يسمح بالوصول إلى آخر المعلومات دائماً.

وهناك تقنيات أخرى مثل برمجيات التطبيقات التي يمكن برمجتها لفحص المواقع المفضلة ليلاً واستقدامها إلى الحاسب المحلي ليصبح بالإمكان تصفحها فيما بعد بسرعة، وبدون الحاجة إلى الانتظار ريثما تجري عملية الاستقدام، ومن هذه البرمجيات WebWhacker و Freeloader، وهي تساعد المستخدمين الذين يعانون من مشاكل في عرض حزمة النقل. وعند استخدام هذه البرمجيات أو غيرها من العناصر الذكية فمن الممكن عرض المعلومات المستقدمة من الإنترنت أو ملخص عنها على جميع المستخدمين بحيث تكون أكثر قابلية للبحث. أخيراً يمكن النظر إلى العناصر الذكية على أنها الصلة بيننا وبين بحر المعلومات الذي هو الإنترنت.

7-3-7 مستقبل تطبيقات الإنترانت

إن مفتاح نجاح الإنترانت في المستقبل هو قدرة وظائف الإنترانت على التكامل مع الأنظمة المثبتة حالياً على الشبكة التعاونية، وخصوصاً التطبيقات التي قد تعمل على حواسيب VAX أو AS400 أو أي أوساط مادية أخرى. ويمكن تحقيق ذلك من خلال استخدام بوابات عبور (واجهات برمجية) من الإنترانت إلى التطبيقات المكتبية أو تطبيقات المخدّم، مما يؤدي بالنتيجة إلى الاستثمار الأمثل للموارد الداخلية المتاحة من قبل المؤسسة ككل. وتعتمد معظم المؤسسات على الحواسيب الشخصية، بمعنى أن أغلب التطبيقات تكون ذات طابع مكتبي. إذن المفتاح هو مكاملة هذه التطبيقات الخاصة في الإنترانت المستقبلية، حيث يصبح المستخدمون أكثر تآلفاً مع تطبيقاتهم المكتبية بمرور الزمن. كما أن المؤسسة وقد وضعت استثمارات معينة في هذه التطبيقات، لذا يكون الحل الأفضل هو الإبقاء على استخدام التطبيقات المكتبية وتعزيزها في الوقت نفسه بالخيارات المتاحة في أنظمة الإنترانت، وكل من شركتي Microsoft و Netscape سوف تنقادان في هذا الاتجاه من التطور على الغالب.

لنفترض أن شركة ما تملك واجهة اتصال مع نظام قواعد معطيات متوارث في الشركة ومتكامل مع شبكة الإنترانت الخاصة بها، فإذا قام جميع المستخدمين في الشركة بتحميل معلوماتهم إلى نظام قواعد المعطيات، فإن الشركة قد تدمج هذه المعلومات في قاعدة معطيات اتصال كبيرة، وتقدم للمستخدم الخيار في استخدام مستعرض الوب للنفاذ إلى النظام، أو إستخدام واجهة النظام الخاصة

للنفاذ إلى نظام قواعد المعطيات، ولكن المهم هو أن يستطيع العاملون الحصول على كامل مجال الوظائف المتاحة بما فيها إمكانية تحديث قاعدة المعطيات من الحواسيب الشخصية.

إن خيار بناء بوابة اتصال بين التطبيقات البرمجية والإنترانت قد لا يناسب الشركات الصغيرة إلاّ إذا كانت تستخدم تطبيقات خاصة بالشركة المنتجة التي تدعم وظائف النفاذ الداخلي والنفاذ عن بعد، حيث ستتطلع هذه الشركات إلى الشركة المنتجة لحل مشاكلها، وستعمل الشركات المنتجة على بناء بوابات اتصال تجعل برامجها تتوافق مع تطبيقات TCP/IP المعيارية، مما يساعد في تحويل أشكال المعطيات إلى أشكال أكثر قابلية للنفاذ عبر الإنترانت، الأمر الذي سيؤدي إلى مكاملة الإنترانت والتطبيقات المكتبية بسرعة وسهولة.

إن نقل المعلومات من التطبيقات المكتبية إلى الإنترانت عملية صعبة، وتتطلب إما برمجيات متخصصة وإمّا بذل قدر لا بأس به من الوقت والجهد والتخصص من قبل الشركة ومبرمجيها. وقد يكون من الأسهل بالنسبة إلى الشركات الكبيرة أن تبدأ من الصفر بحل يقوم على إنترانت محلية، أما بالنسبة للشركات الصغيرة التي قد تكون مهددة مالياً فإنها تحتاج إلى التفكير بروية بالحلول المكنة لتجنب انهيارات كبيرة في نظام المعلومات وضياعات في الاستثمار.

ونحن الآن بصدد الانتقال إلى مجال جديد كلياً بفضل الإنترانت والتطبيقات التي كانت تنفّذ سابقاً على المخدّم في مكان مركزي حيث يجري تخزين ومعالجة المعطيات، فبرنامج الزبون أو الطرفية المستخدمة من قبل المستخدم أصبحا اليوم نافذة إلى هذا المخدّم. واليوم فإن النافذة الأكثر شيوعاً هي الحاسوب الشخصي، ولكن هذا الأمر قد يتغير بالظهور التجاري لما يسمى بـ "حاسوب الشبكة"، وهذا الحاسوب هو آلة مستخدم مزودة بأقل ما يمكن من الإضافات لتعمل كنافذة تسمح بالنفاذ إلى الإنترانت، وقد يسمى أحياناً بـ "طرفية الإنترنت"، وسيُدخل هذا المفهوم إلى الهاتف الخليوي أو إلى أي جهاز رقمي شخصي مساعد ليعمل كنافذة أو بوابة عبور إلى الإنترانت حيث يجري التنفيذ الفعلي للبرامج على المخدّمات، وتُرسل معطيات الخرج فقط إلى الزبون لتُعرض هناك.

وبدلاً من امتلاك حاسوب شخصي بنظام تشغيل تقليدي، يمكن الحصول على آلة مصممة خصيصاً لتنفيذ تطبيقات الشبكة أو خدمات TCP/IP. تتمثل وظيفة هذه الآلة بالنفاذ إلى المخدّم للحصول على المعطيات لمعالجتها بطريقة أو بأخرى ومن ثم إرسالها إلى المخدّم. على سبيل المثال قد لا يحتوي حاسوب الشبكة على قرص صلب وإنما يستطيع النفاذ فقط إلى الإنترانت أو الإنترنت أو أي شبكة يُوصل إليها. وقد يستقدم هذا الحاسب بريمج Java (Applet) للقيام بالمعالجة الضرورية من جهة الزبون وعند انتهاء هذا البريمج من التنفيذ فإنه سيحذف من ذاكرة الحاسب، وقد يعاد استقدام هذا البريمج أو أي بريمج آخر عند الضرورة لتنفيذ المهام المتتالية.

حواسيب Palm-top

يستطيع هذا الحاسب النفاذ إلى موارد الإنترانت عبر موديم لاسلكي، ويمكن أن يعمل كهاتف صوتي، وبما أنه من الممكن جمع كل هذه التقنيات في كيان واحد، فإن هذا الحاسوب يمكن أن يتصرف كزبون من دون الحاجة إلى ميزات خاصة، لأن العمل على الموارد يجري على المخدّم البعيد ولكننا نحتاج إلى وصلة سريعة للقيام بالعمل بفعالية.

المؤتمرات عن بعد

سوف تصبح المؤتمرات عن بعد شبه مجانية مقارنةً بتكلفة المكالمات البعيدة، حيث أن الاتصالات ستنتقل عبر الإنترانت إلى المخدّم الذي سيقوم بدوره بإجراء مكالمة محلية مع المستقبل، أو يتصل مع برمجية مبيتة في برمجيات المستقبل، وفي الحالة الأخيرة فإن نقل المكالمة سيشكل تخاطباً بين حاسبين وفي هذه الحالة تظهر عدة أسئلة حول من سيتحمل نفقة إقامة مثل هذا النظام، إذ أن شركة الهاتف غير مهيأة بأي وسيلة لمراقبة هذا النظام بفعّالية، وإذا كان مالكو المخدّمات هم الذين سينفقون لتقديم هذه الخدمة، فإن النظام بأكمله سيكون عرضة للعديد من الاتصالات الدخيلة والتي قد تؤثر على كفاءة النظام.

تمثل الحالة الثانية تحقيقا لتقنية وليدة مستخدمة حاليا على الإنترنت، على الرغم من عدم جاهزيتها للبيئة التعاونية: وهي تطبيقات الإنترنت الهاتفية، حيث أن استخدام هذه التقنية يجري بتسجيل رسائل المستخدمين وتحويلها إلى شكل خاص مثل wav. أو au.، ومن ثم ترسل إلى المستقبل الذي يقوم بإعادة تحويلها إلى صوت باستخدام برمجيات معينة لسماعها، وحاليا فإن نوعية الصوت المعتمدة ليست معيارية تماما، وستصبح كذلك عند الوصول إلى مستوى مقبول في سرعة النقل وعرض الحزمة، ويمكن عندئذ تحقيق حلول أفضل للمؤتمرات عن بعد باستخدام الصوت والصورة.

وبما أن الأعمال تنحو بصورة متزايدة نحو الانتشار العالمي فإن الخدمة السابقة التي قد تقدمها الإنترانت بفعالية أكبر سوف تساعد في إبقاء أسعار الاتصالات العالمية منخفضة، ومن البرمجيات التي تقوم بهذه الخدمة على الإنترنت نجد IP Phone و Web Phone و Internet Phone.

من وظائف المؤتمرات عن بعد والتي تدخل في مضمار حديثنا هناك وظيفة تسجيل بعض الإحصائيات عند نهاية المكالمة في قاعدة معطيات مركزية، مما يؤكد حدوث مكالمات معينة مع معلومات عن مدتها وتكلفتها وما إلى ذلك من معلومات. ومن الممكن تسجيل المكالمة وحفظها وربطها مع أحد الجداول في قاعدة المعطيات، بحيث يمكن العودة إلى يوم معين لرؤية ما تم فيه من مكالمات مع إمكانية إعادة سماعها، وبما أن تقنيات ضغط وترميز الصوت تصبح أكثر تقدما فقد نلاحظ ميلا نحو تسجيل كافة المكالمات الهاتفية، إضافة إلى رسائل البريد الصوتي على مخدم ما في مكان معين من الإنترانت، ولهذا الأمر العديد من التطبيقات القانونية التي يمكن تطبيقها للإقرار بصحة هذه العملية قانونيا. والخطوة التالية في تقدم هذه التكنولوجيا هي التعرف على الصوت في الزمن الحقيقي، والتي ستسمح بتحويل المكالمة آليا إلى نص مكتوب يمكن إرساله إلى كافة المشاركين، أو قد تبث المحادثة مع النسخة النصية لمستخدمين آخرين يرغبون بمراقبة وسماع ما يحدث في المكالمة.

إن التقنية السابقة موجودة حاليا بدرجات متفاوتة من الفعالية ولكن أيا منها ليس على الدرجة الملائمة من الفعالية كما أنها غير قابلة للتطبيق التجاري، وفي المستقبل القريب فإن التطور في البنية المادية والبرمجية قد يجعل هذا النوع من الأنظمة ممكنا في الشركات المتوسطة الحجم على الأقل.

4-7 إكسترانت Extranet

تقوم شبكات إكسترانت على أسس ومفاهيم الإنترانت، ولكن بدلا من ربط المستخدمين الداخليين فإن شبكات إكسترانت تربط زبائن المؤسسة والممولين وشركاء الأعمال الخارجيين.

إن ما يميز تكنولوجيا الإنترانت لا يتعلق بما يمكن أن تقدمه وإنما بالذي سوف تقودنا إليه، وكل ما قد عرضناه في هذا الكتاب حتى الآن لا يمثل الشكل المثالي والكامل، وكل ما يتعلق بتوظيف تكنولوجيا الإنترانت في مجال الأعمال والمؤسسات لا يتعدى كونه نقطة بداية، والحقيقة هي أنه على الرغم من أن الإنترانت سوف تنقص من مشكلات التكرار وعدم الكفاءة في المؤسسات، فإن العديد من هذه المشكلات سيبقى، وسيأتي الاختبار الحقيقي لهذه التكنولوجيا عندما تكون كل المعلومات ذات الصلة بكيان ما مكاملة ضمن مخزن وحيد للمعلومات ذي واجهات تخاطبية متعددة للنفاذ إليه.

لنأخذ مثلا شركة لإنتاج شاشات الحواسيب، يملك هذا النوع من الشركات الكثير من المعلومات، مثل المنتجات المروجة وطلبات الشراء وفواتير تقارير الأرباح، ولربما يشبه نظام إدارة المعلومات في هذه الشركة النظام التالي: لدى الشركة موقع وب يحتوي على معلومات تتعلق بكيفية الاتصال بالشركة، إضافة إلى معلومات عن المواد المروجة، وقد تملك الشركة شبكة إنترانت تضم معلومات عن الموارد البشرية في الشركة، وقاعدة معطيات للمخزون وتطبيقات تعاونية أخرى، وفيما يتعلق ببناء الفواتير وطلبات الشراء وتدوين المبيعات فإنها قد تكون مؤتمتة في تطبيقات مستقلة.

لنعتبر الآن شبكة إكسترانت هي مزج لشبكة الإنترانت الموجودة مسبقا مع الإنترنت، فعندما يطلب أحد الباعة شراء عدد من الشاشات التي تنتجها الشركة فإن إكسترانت تنظر إلى موقع الشركة وتتحقق من المواصفات المطلوبة وبعد ذلك تتأكد من الأسعار الحالية وتوفر الطلب، وكزبون جديد تدخل إكسترانت إلى مخزن المعلومات وتضع الطلبية ؛ تدخل هذه المعلومات أتوماتيكيا في قاعدة بيانات معلومات اتصال الشركة المنتجة ويوضع الطلب، ثم تطبع علامة الشحن وتسجل الصفقة في المحاسبة وتحدث قاعدة بيانات المخزون. تبنى الفاتورة وترسل، ويجري إعلام موردي الأجزاء بالطلبية وترسل الأجزاء الجديدة. توفر إكسترانت طرقا بسيطة وفعالة وسريعة لتقنيات إدارة

المعلومات والتي ستؤدي إلى التغيير الأكثر شمولية في طريقة إدارة العمل. إن مخزن المعلومات البسيط الذي يعمل عبر مختلف الأوساط ويوفر عدة واجهات للتخاطب وفق مستويات نفاذ متعددة يعتبر الخطوة القادمة في تكنولوجيا المعلومات. وسيصبح التكرار في المعلومات والخليط الورقي وإدخال البيانات جزءا من الماضي. سيقل عدد مواقع الوب الثابتة المحتوى وسيزداد عدد المواقع التي تقدم الخدمات الفورية التفاعلية. وسوف تصبح شبكة الوب العالمية أحد مداخل الشركات والمؤسسات، وسوف تحل مكان المكالمات الهاتفية والفاكسات وحتى واجهات عرض المنتجات في المحلات التجارية. ولن نعود مضطرين لانتظار الأوراق في البريد أو الانتظار لوضع طلبية ما.

وعند مكاملة كافة مخازن المعلومات هذه، فمن المتوقع أن نرى نقلة في مجال الخدمات الآنية، وستصبح الإنترانت أداة للعمل والتجارة أكثر من كونها وسطا للترفيه، كما قد نتوقع ضعف سيطرة بعض الشركات الكبرى في السوق أمام الشركات الأكثر فطنة والتي قد تخاطر باتباع تكنولوجيات المعايير المفتوحة، وقد يكون العاملون في توحيد الأنظمة ومطورو البرمجيات هم الأشخاص الرابحون في المستقبل، وعلى كل حال فإن الأمور ستكون كثيرة التقلب وسيكون من المتع مراقبة ما سيحدث.

المراجع المستخدمة في الكتاب

1- الكتب

1. David Garrett et al.

Intranets Unleashed

SAMS.NET, 01-SEP-1996.

2. Fred HALSALL

Data Communications, Computers, Networks and Open Systems

ADDISON-WESLEY Publishing Company 1992.

3. Rick Casselberry

Running a Perfect Intranet

QUE, 01-SEP-1996.

4. Scott Zimmerman.

Building an Intranet with Windows NT 4

SAMS.NET, 01-AUG-1996.

5. Laurent Toutain

Réseaux locaux et Internet: des protocols à l'nterconnexion.

2e édition revue et augmenté

HERMES Science Publication, Paris, 1996, 1999.

6. Preston Gralla
How Intranet Works
ZDPRESS, 01-NOV-1996.

7. Patrick Smith & Steve Guengerich
Client/Server Computing, Second Edition
SAMS, 01-FEB-1994.

2- الوثائق

1. Compaq White Paper
Intrusion Detection in the Enterprise Network: Managing Hackers-Related Risk
Compaq Computer Corporation, March 1998.

2. Check Point Technical White Paper
Virtual Private Network Security Components
March 23, 1998.

3. 3COM Technical White Papers
Private Use of Public Networks for Enterprise Customers
3COM Corporation, 1998.

3- معظم مواقع الإنترنت المذكورة في الكتاب

عناوين صدرت في سلسلة الرضا للمعلومات

اسم الكتاب	المؤلف	تاريخ النشر
١- بيئة النوافذ WINDOWS 3.11	م. أحمد شربك	١٩٩٤
٢- مبادئ الصيانة والشبكات	م. عبد الله أحمد	١٩٩٤
٣- معالجة النصوص MS WORD 6.0	د. هيثم البيطار	١٩٩٥
٤- ادخل إلى عالم WINDOWS 95	م. مهيب النقري	١٩٩٦
٥- قواعد البيانات MS ACCESS	زياد كمرجي - بيداء الزير	١٩٩٧
٦- توابع وماكروات في MS EXCEL 97	أ. زياد كمرجي	١٩٩٧
٧- مرجع تعليمي شامل لبرنامج معالجة النصوص MS WORD 97	د. هيثم البيطار	١٩٩٧
٨- مرجع تعليمي شامل في MS EXCEL 97	أ. زياد كمرجي	١٩٩٧
٩- مرجع تعليمي شامل في صيانة الحواسب الشخصية	م. عبد الله أحمد	١٩٩٨
١٠- مرجع تعليمي في برنامج الرسم والتصميم الهندسي AUTOCAD 14	م. احسان مردود	١٩٩٨
١١- المرجع التدريبي الشامل لـ WINDOWS 98	م. إياد زوكار	١٩٩٨
١٢- ادخل إلى عالم WINDOWS 98	م. مهيب فواز النقري	١٩٩٨
١٣- الإنترنيت وإنترانيت وتصميم المواقع	م. عبد الله أحمد	١٩٩٨
١٤- تكنولوجيا المعلومات على أعتاب القرن الحادي والعشرين	هاني شحادة الخوري	١٩٩٨

Converted by Tiff Combine - (no stamps are applied by registered version)

١٥-الإدارة الاستراتيجية للشركات والمؤسسات د.يونس حيدر ١٩٩٩

١٦-نظام الـ ISO 9004-1 م.محمد حسن -م.بسام عزام ١٩٩٩

١٧-القائد المفكر حافظ الأسد
والمشروع التنموي الحضاري د.رياض عواد-أ.هاني الخوري ١٩٩٩

١٨- فن إدارة البشر د. محمد مرعي مرعي ١٩٩٩

١٩- المرجع الشامل لتعليمات
برنامج AUTOCAD م. احسان المردود -م. وهبي معاد ١٩٩٩

٢٠- الدعاية والتسويق ومعاملة الزبائن م. حنا بللوز ١٩٩٩

٢١- المعلومياء (المعلوماتية)
ظروفها وآثارها الاقتصادية - الاجتماعية د. معن النقري ١٩٩٩

٢٢- المرجع الشامل لبرنامج
3D STUDIO MAX - الجزء الأول م. جورج عطا الله بركات ١٩٩٩

٢٣- دليل الجودة في المؤسسات والشركات د. طلال عبود-أ.ماهر العجي ١٩٩٩

٢٤-المرجع المفيد في علم شبكات الحواسيب
د.معتصم شفا عمري ١٩٩٩

٢٥- ادخل إلى عالم ORACLE 8 م. مهيب النقري ١٩٩٩

٢٦- أسس إدارة الموارد البشرية د. محمد مرعي مرعي ١٩٩٩

٢٧- تعلم برنامج إدارة قواعد البيانات أ. زياد كمرجي - م. مهيب النقري ١٩٩٩

٢٨- الدليل الشامل لأساسيات
الحاسوب والمعلوماتية م. عبد الله أحمد ١٩٩٩

٢٩-(الكذبات العشر للعولمة د. عدنان سليمان ١٩٩٩

٣٠- بعض مسائل الاقتصاد اللاسياسي د. مطانيوس حبيب ١٩٩٩

٣١- دليل إعادة تنظيم المؤسسات د. محمد مرعي مرعي ١٩٩٩

٣٢- الدراسات التسويقية ونظم معلومات التسويق	د. طلال عبود - د. حسين علي	١٩٩٩
٣٣- مدخل إلى المعلوماتية الطبية	م. جورج بركات - أ. هاني الخوري	١٩٩٩
٣٤- الدعاية والتسويق وفن التعامل مع الزبائن - جزء ٢	م. حنا بللوز	١٩٩٩
٣٥-تعلم كل شيء عن جافا	م.مهيب النقري	١٩٩٩
٣٦- مبادئ العمل السكرتاري باستخدام برنامج OUTLOOK	بيداء الزير	١٩٩٩
٣٧- أساسيات الإدارة المالية الحديثة	د. دريد درغام	١٩٩٩
٣٨- دليل التشخيص وتحديد الأهداف ووضع الخطط في المؤسسات	د. محمد مرعي مرعي	١٩٩٩
٣٩- التسويق وإدارة الأعمال التجارية	م. إياد زوكار	١٩٩٩
٤٠- أجهزة التحكم القابلة للبرمجة PLC	م. عبده هلاله	١٩٩٩
٤١- أمثلة وحالات عملية MS. EXCEL	م. إياد زوكار- م. نهال زركلي	٢٠٠٠
٤٢- المرجع الشامل لبرنامج 3D Studio Max - الجزء الثاني	م. جورج بركات	٢٠٠٠
٤٣- الأساليب الحديثة في التسويق	د. حسين على	٢٠٠٠
٤٤- مرجع في صيانة الحواسب الشخصية	م. عبد الله أحمد	٢٠٠٠
٤٥- البرمجة في Access 2000	د. باسل الخطيب	٢٠٠٠
٤٦- دليل المحترفين إلى **Corel Draw 9**	م. سامر سعيد - م. حنان مسلّم - م. مصعب النقري	٢٠٠٠
٤٧- المرجع الشامل في برنامج معالجة النصوص MS Word 2000	د. هيثم البيطار - بوليت صارجي	٢٠٠٠

عناوين ستصدر قريباً

اسم الكتاب	المؤلف	تاريخ النشر المتوقع
١- البحث عن المعلومات في الإنترنت	د. عمّار خير بك	٢٠٠٠
٢- التسويق عبر الانترنت	د. طلال عبود	٢٠٠٠
٣- الحساسات وطرق الربط إلى أنظمة التحكم المبرمج	م. عبده هلاله	٢٠٠٠
٤- نظام الشبكات WINDOWS NT	م.احسان مردود	٢٠٠٠
٥- تقنية المعلومات في إدارة الشركات	م. قاسم شعبان	٢٠٠٠
٦- تصميم المواقع WEB DESIGN	م.عبد الله أحمد	٢٠٠٠
٧- EXCEL 2000 - الجزء الثاني	م. إياد زوكار- م. محمد الضمّاد	٢٠٠٠
٨- المعلوماتية الطبية	د.نبيل دك الباب	٢٠٠٠
٩- أساسيات الإدارة المالية الحديثة - ج٢	د. دريد درغام	٢٠٠٠
١٠- مرجع أساسيات الحوسبة ج٢	إشراف م. قاسم شعبان شادي سيدا	٢٠٠٠
١١- المرجع الأساسي في MICROMEDIA DIRECTOR 7	أ. وائل جلال	٢٠٠٠
١٢- إدارة الابتكار والابداع	أ. رعد الصرن	٢٠٠٠
١٣- تقنية المعلومات في إدارة الشركات	م. قاسم شعبان	٢٠٠٠
١٤- كتاب Autocad 2000	م. احسان مردود - م. وهبي معاد	٢٠٠٠
١٥- كتاب الحساسات وطرق الربط إلى أنظمة التحكم المبرمج	م. عبده هلاله - م. عامر عبود	٢٠٠٠
١٦- سلسلة الرضا لتبسيط علوم الحاسوب	م. مهيب النقري - د. معتصم شفا عمري	٢٠٠٠











سلسلة الرضا للمعلومات
دار الرضا للنشر

هذا الكتاب

يُعتبر انتشار وسيطرة الإنترنت والتطبيقات البرمجية العاملة عليها والتي نتجت عن نجاح الإنترنت وشعبيتها هي التي أنتجت الإنترانت وهيأت مستقبلها المتألق.

يتناول هذا الكتاب عرضاً لتكنولوجيا الإنترانت من مختلف الجوانب ابتداءً من البنية التحتية وصولاً إلى التطبيقات التعاونية والخدمات التي توفرها شبكات الإنترانت وانعكاساتها على البنية التنظيمية وطريقة إدارة المؤسسات، إضافةً لمناقشة مختلف الأمور المتعلقة بأمن شبكات الإنترانت، كما يعرض مختلف المعلومات التقنية اللازمة لبناء وإدارة شبكات الإنترانت.

مبتدئ متوسط متقدم

Cover by : Hot Design